Terms Of Contract

PRIVATE & CONFIDENTIAL

TEL: +65 6817 8204
FAX: +65 6817 8205
EMAIL: info@gls.global

Global Legal Solutions™
37 Beach Road, #02-01, Singapore 189679
www.gls.global

DATA PROCESSING AGREEMENT

Version No.	**GLS Draft 1**
Release Date	**5 March 2020**
Author	**GLS**

Table of Contents

AGREED TERMS 4

1. DEFINITIONS 4
2. INTERPRETATION 4
3. ROLES & RESPONSIBILITIES 4
4. PROCESSING INSTRUCTIONS 5
5. DATA PROTECTION IMPACT ASSESSMENT 5
6. TECHNICAL & ORGANISATIONAL MEASURES 5
7. UNAUTHORISED DATA EVENTS 6
8. INTERNATIONAL DATA TRANSFERS 6
9. PROTECTED DATA NOTIFICATIONS 7
10. DATA SUBJECT ACCESS REQUEST 7
11. DELETION OR RETURN OF PROTECTED DATA 8
12. RECORDS & AUDIT 8
13. LIMITATION OF LIABILITY 8
14. INDEMNITIES 9
15. TERMINATION 9
16. DATA PROTECTION OFFICER 9
17. SUPPLIER PERSONNEL 10
18. SUB-PROCESSING 10
19. PROJECT AND DPA RELATIONSHIP 10
20. AMENDMENTS 10
21. MISCELLANEOUS PROVISIONS 11

SCHEDULE 1 | DEFINITIONS 14

1. DEFINITIONS 14

SCHEDULE 2 | ESSENTIAL PROCESSING PARTICULARS 18

1. REQUIRED PROCESSING 18

2. PROCESSING INSTRUCTIONS 18

SCHEDULE 3 | SECURITY MEASURES 19

1. SECURITY MEASURES 19

THIS DATA PROCESSING AGREEMENT is made on this [●] day of the month of [●] [●]:

Between

(1) [●], a company incorporated under the laws of [●] with registration number [●] and having its registered office address at [●] (“**Client**”); and

(2) [●], a company incorporated under the laws of [●] with registration number [●] and having its registered office address at [●] (“**Supplier**”).

(collectively, the “**Parties**” and each, a “**Party**”).

RECITALS

A. The Parties are currently engaged in a Project in relation to which Personal Data provided by the Client is to be processed by the Supplier.

B. Both Parties would like to ensure that in performing the Project, each Party is compliant with their respective obligations under Data Protection Laws.

C. This DPA is intended to ensure that as the Parties perform their obligations in connection with the Project insofar as it involves the Processing of Protected Data in a manner that complies with Data Protection Laws.

IT IS HEREBY AGREED as follows:

<u>AGREED TERMS</u>

1. DEFINITIONS

1.1 The defined terms in this DPA shall have the meaning ascribed to them in **Schedule 1 (Definitions)**.

2. INTERPRETATION

2.1 In this DPA, the following rules of interpretation shall apply:

2.1.1 references to Schedules and Annexures are (unless otherwise provided) references to the schedules and annexures of this DPA;

2.1.2 a reference to a Clause or Paragraph is a reference to the clause or paragraph of this DPA;

2.1.3 references to a “day”, “month” or “year” are references to a “day”, “month” or “year” of the Gregorian calendar; and

2.1.4 a reference to “including” and its other grammatical forms shall be construed without limitation.

3. ROLES & RESPONSIBILITIES

3.1 Unless otherwise specified in **Schedule 2 (Essential Processing Particulars)**, the Parties acknowledge and agree that for the purposes of Protected Data under Data Protection Laws:

3.1.1 the Client is the Data Controller and shall comply with all Data Protection Laws in respect of the Protected Data and its obligations under this DPA; and

3.1.2 the Supplier is the Data Processor and shall comply with all Data Protection Laws in connection with the Processing of Protected Data and performance of its obligations under this DPA.

4. PROCESSING INSTRUCTIONS

4.1 The Supplier shall only Process the Protected Data on behalf of the Client strictly in accordance with the Processing Instructions, unless required to do otherwise by Applicable Law.

4.2 Where Applicable Law requires the Supplier to process the Protected Data other than in accordance with the Processing Instructions then the Supplier shall:

4.2.1 promptly notify the Client that Applicable Law requires it to Process the Protected Data in a manner contrary to the Processing Instructions; and

4.2.2 provide the above notification to the Client before such Processing actually commences unless Applicable Law itself actually prohibits such notification, for example, on grounds of public interest.

4.3 For the purposes of this DPA, the Processing Instructions must always be provided by the Client to the Supplier in a comprehensive written format such as is set out in **Schedule 2 (Essential Processing Particulars)**.

4.4 As at the date of this DPA, the Processing Instructions are as set out in **Schedule 2 (Essential Processing Particulars)** and may not be changed other than by written agreement between the Parties.

4.5 The Supplier shall, unless prohibited by Data Protection Laws, notify the Client immediately if it considers that any of the Processing Instructions infringe the Data Protection Laws.

4.6 [**Client friendly:** Where the Supplier believes that the Processing Instructions are incompatible and/or incomplete for what is required to give effect to the Project, the Supplier may notify the Client and the Parties can discuss the same in good faith.]

5. DATA PROTECTION IMPACT ASSESSMENT

5.1 Prior to commencing any Processing of Protected Data, the Supplier shall use [reasonable/best] endeavours to assist the Client in the preparation of any Data Protection Impact Assessment, including:

5.1.1 a systematic description of the envisaged Processing operations and the purpose of Processing;

5.1.2 an assessment of the necessity and proportionality of the Processing operations in relation to the Project and/or the services performed by the Supplier for the Client;

5.1.3 an assessment of the risks to the rights and freedoms of Data Subjects posed by the contemplated Processing; and

5.1.4 the measures envisaged to address the risks referenced in Clause 5.1.3, including safeguards, security measures and mechanisms to ensure the protection of Protected Data.

6. TECHNICAL & ORGANISATIONAL MEASURES

6.1 The Supplier shall implement and maintain, at its sole cost and expense, appropriate technical and organisational measures in relation to its Processing of Protected Data as is required by Data Protection Laws.

6.2 Without prejudice to the generality of Clause 6.1, the Supplier shall implement the Protective Measures as are necessary to:

6.2.1 ensure the protection of the Data Subjects’ rights;

6.2.2 prevent an Unauthorised Data Event in relation to the Protected Data; and

6.2.3 ensure a level of security in respect of Protected Data being Processed as is appropriate to the risks presented by the Processing.

6.3 When meeting its obligations under Clause 6.2, the Supplier shall, without limitation, take into account the following considerations:

6.3.1 the nature of the Protected Data;

6.3.2 the harm that might result from an Unauthorised Data Event;

6.3.3 the state of technological development; and

6.3.4 the cost of implementing any Protective Measures.

6.4 The Supplier shall provide appropriately secure facilities so that the Client can transfer all Protected Data to the Supplier for the purposes of this DPA.

7. UNAUTHORISED DATA EVENTS

7.1 In respect of any Unauthorised Data Event, the Supplier acknowledges and agrees that it shall:

7.1.1 notify the Client of Unauthorised Data Event without undue delay (but in no event later than 1 Business Day after becoming aware of such breach); and

7.1.2 provide the Client without undue delay with such details as the Client reasonably requires regarding:

(a) the nature of the Unauthorised Data Event;

(b) any investigations into such Unauthorised Data Event; and

(c) any measures taken, or that the Supplier recommends, to address the Unauthorised Data Event.

7.2 The Supplier shall use best endeavours to monitor and guard against the occurrence of attempted Unauthorised Data Events and to eliminate the potential of any re-occurrence of any Unauthorised Data Events notified under Clause 7.1.1.

8. INTERNATIONAL DATA TRANSFERS

8.1 The Supplier shall not transfer Protected Data [to any International Recipient]/[out of the Territory] without obtaining the Client's prior written approval, which shall not be given unless the following conditions are and will be met:

8.1.1 appropriate safeguards exist in relation to the transfer that guarantee no violation of Data Protection Laws shall occur, the adequacy of such guarantee to be as determined by the Client in its sole discretion;

8.1.2 the Data Subject shall still have enforceable rights and effective legal remedies in respect of the Protected Data that are no less stringent than if the transfer did not occur;

8.1.3 the Supplier provides adequate protection to any Protected Data such that all of the rights enjoyed by the Client under this DPA remain enforceable;

8.1.4 the Supplier shall continue to be able to comply with all of its obligations under or in connection with this DPA and Data Protection Law without any compromise whatsoever;

8.1.5 the Supplier shall continue to strictly comply with the Processing Instructions in relation to the Processing of Protected Data; and

8.1.6 the deletion or return of Protected Data (and any copies of the same) on termination of this DPA in accordance with the Processing instructions, unless the Supplier is required under Data Protection Laws to retain the same.

9. PROTECTED DATA NOTIFICATIONS

9.1 The Supplier shall promptly (and in any event within 1 Business Day) inform the Client in writing and provide the Client with all relevant information where it:

9.1.1 receives a complaint connected with its Processing of the Protected Data and provide the Client with full details of such complaint;

9.1.2 receives a Data Subject Request (or a purported Data Subject Request);

9.1.3 receives a request to rectify, block or erase any Protected Data;

9.1.4 receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Laws;

9.1.5 receives any communication from any Supervisory Authority in connection with Protected Data Processed under this DPA;

9.1.6 receives a request from any Third Party for disclosure of Protected Data where compliance with such request is required or purported to be required under Data Protection Laws; and

9.1.7 becomes aware of an Unauthorised Data Event.

9.2 The Supplier acknowledges and agrees that its obligation under Clause 9.1.1 extends to providing the Client with all subsequently available information relevant to the matters under Clauses 9.1.2 to 9.1.7.

10. DATA SUBJECT ACCESS REQUEST

10.1 The Supplier shall use [best/reasonable] endeavours to assist the Client in the fulfilment of the Client's obligations to respond to Data Subject Requests relating to Protected Data.

10.2 The Supplier shall (at no cost and expense to the Client):

10.2.1 promptly record and then refer all Data Subject Requests it receives to the Client within 3 days of receipt of the request;

10.2.2 provide such information and cooperation and take such action as the Client requests in relation to a Data Subject Request, within the timescales required by the Client; and

10.2.3 not respond to any Data Subject Request or complaint without the Client's prior written approval.

10.3 The Supplier shall (and shall ensure that its Personnel shall) provide reasonable cooperation to the Client so that the Client can comply with its obligations under the Data Protection Laws.

10.4 The Supplier shall provide the Client with full assistance in relation to either Party's obligations under Data Protection Laws and any complaint, communication or request made under Clauses 9 and 10.

10.5 Without prejudice to the generality of Clause 10.4, the Supplier shall promptly provide the Client with:

10.5.1 full details and copies of the complaint, communication or request;

10.5.2 such assistance as is reasonably requested by the Client to enable the Client to comply with a Data Subject Request in accordance with the Data Protection Laws;

10.5.3 any Personal Data it holds in relation to a Data Subject;

10.5.4 assistance as requested by the Client following any Unauthorised Data Event; and

10.5.5 assistance as requested by the Client in relation to any request from or any consultation by the Client with any Supervisory Authority.

11. DELETION OR RETURN OF PROTECTED DATA

11.1 The Supplier shall promptly, at the Client's written request, either securely delete or securely return all the Protected Data to the Client in such form as the Client reasonably requests after the earlier of:

11.1.1 the end of the provision of the relevant services related to Processing; or

11.1.2 once Processing by the Supplier of any Protected Data is no longer required for the purpose of the Project.

11.2 The Supplier shall promptly inform the Client where Protected Data may not be deleted without violating Data Protection Laws.

12. RECORDS & AUDIT

12.1 The Supplier shall maintain complete and accurate records and information for the purposes of demonstrating its compliance with its obligations under this DPA.

12.2 During the Term, the Client may, at its own cost, Audit the performance of the Supplier's obligations under this DPA in accordance with this Clause 12 upon giving [10] Business Days' notice.

12.3 The Supplier shall fully co-operate with the Client and its Auditors and promptly provide such Auditors with reasonable access to the records and information under Clause 12.1.

12.4 Where the Audit shows that the Supplier has not performed its obligations under this DPA, then the Supplier shall:

12.4.1 pay the Client's reasonable Audit costs and expenses; and

12.4.2 promptly (and in any event within not more than [15] Business Days) rectify the breaches identified by the Audit or otherwise show evidence of remedial measures undertaken to avoid a reoccurrence of such breaches.

12.5 The Supplier acknowledges and agrees that a breach of Clause 12.4 shall be a Material Breach.

12.6 The Client shall be entitled to exercise its Audit rights under this Clause 12 not more than 2 times each Contract Year, provided however that any Audit revealing non-performance by the Supplier shall not be counted against this entitlement.

13. LIMITATION OF LIABILITY

13.1 This Clause 13 is intended to apply to the allocation of liability for Data Protection Losses as between the Parties, including with respect to compensation to Data Subjects, except:

13.1.1 to the extent not permitted by Applicable Law (including Data Protection Laws); and

13.1.2 that it does not affect the liability of either Party to any Data Subject and/or their Personnel.

13.2 Neither Party shall limit (or attempt to limit) its liability with respect to any individual's data protection rights under this DPA or otherwise.

13.3 [**Supplier friendly:** The Supplier's total liability for Data Protection Losses arising out of or in connection with this DPA shall not in any event whatsoever exceed [insert cap which will depend on nature/relationship of parties and Project].]

13.4 [**Supplier friendly:** Any regulatory penalties incurred by the Supplier in relation to Protected Data shall count toward and reduce the Supplier's liability under this DPA as if it were liable to the Client under this DPA.]

13.5 [**Supplier friendly:** Clause 13.2 shall be limited to the extent that such regulatory penalties arise as a result of, or in connection with, the Client's:

13.5.1 failure to comply with its obligations under this DPA; or

13.5.2 breach of any applicable Data Protection Laws.]

13.6 [**Client friendly:** The Supplier shall, where requested by the Client, obtain insurance from a reputable insurer acceptable to the Client, that covers its total potential liability to the Client under or in connection with this DPA.]

13.7 [**Client friendly:** Where Clause 13.6 applies and where requested by the Client, the Supplier shall within [●] days of the Client's request provide the Client with certificates of insurance, receipts for the current year's premiums, and any other proof of insurance the Client may reasonably require.]

14. INDEMNITIES

14.1 [**Client friendly:** The Supplier shall fully indemnify the Client for any Data Protection Losses arising out of or in connection with an Unauthorised Data Event or any breach of this DPA.]

14.2 [DN: If you can get the above indemnity then great – but please note that due to the severity of consequences associated with GDPR breaches, companies are increasingly unable/unwilling to accept indemnities in respect of Data Protection breaches.]

14.3 [DN: The above indemnity is useful where the relationship between you (as the Client) and the third party processing your data is such that data protection breaches can occur easily, despite your best efforts, due to the ubiquity of means to transfer mass amounts of data and the propensity of human error.]

15. TERMINATION

15.1 The Client may terminate this DPA with immediate effect where:

15.1.1 the Supplier is in Material Breach; and/or

15.1.2 it has exercised any right that it may have to terminate its participation in the Project.

16. DATA PROTECTION OFFICER

16.1 Where required by the Data Protection Laws, each Party shall designate its own data protection officer and communicate the identity of such officer to the other Party.

16.2 Each Party shall ensure that their data protection officer is appropriately trained and qualified to perform such role as required under Data Protection Laws.

17. SUPPLIER PERSONNEL

17.1 The Supplier acknowledges and agrees that it shall:

17.1.1 inform its Personnel of the Supplier’s duties under this DPA;

17.1.2 ensure that its Personnel are subject to appropriate confidentiality undertakings with the Supplier or Sub-processor (if a sub-processor has been notified to and approved by the Client);

17.1.3 inform its Personnel that the Protected Data they Process is strictly confidential;

17.1.4 ensure that its Personnel do not publish, disclose or divulge any Protected Data to any Third Party, unless authorised by the Client in writing or otherwise permitted under this DPA; and

17.1.5 ensure that its Personnel have undergone training in the use, care, protection and handling of Protected Data to the Supplier’s satisfaction.

17.2 For the purposes of Clause 17.1.2, the Supplier acknowledges and agrees that:

17.2.1 all non-disclosure agreements to be executed by the Supplier’s Personnel shall be subject to the Client’s approval; and

17.2.2 the Supplier shall provide the Client a copy of any non-disclosure agreement referred to under Clause 17.2.1 upon the Client’s request.

18. SUB-PROCESSING

18.1 Before allowing any Sub-processor and/or its Personnel to Process any Protected Data related to this DPA, the Supplier shall:

18.1.1 notify the Client in writing of the intended Sub-processor and the contemplated Processing;

18.1.2 obtain the written consent of the Client which may be withheld by the Client in its sole and absolute discretion;

18.1.3 enter into a written agreement with the Sub-processor giving effect to the terms set out in this DPA (where applicable) such that they apply to the Sub-processor; and

18.1.4 provide the Client with such information regarding the Sub-processor as the Client may reasonably require.

18.2 The Supplier acknowledges and agrees that it shall be fully liable for all acts and/or omissions of any of its Sub-processors.

19. PROJECT AND DPA RELATIONSHIP

19.1 Any claims against the Supplier or its Affiliates under this DPA in relation to the Protected Data in connection with the Project shall be brought solely against the entity that is a party to this DPA.

20. AMENDMENTS

20.1 The Client shall be entitled to, at any time on not less than 30 Business Days’ notice, revise this DPA by replacing it with any:

20.1.1 applicable controller-to-processor standard clauses; or

20.1.2 similar terms forming part of an applicable certification scheme (which shall apply when incorporated by attachment to this DPA).

20.2 The Supplier acknowledges and agrees that the Client shall be entitled to, at any time on not less than 30 Business Days' notice, amend this DPA to ensure that it complies with any guidance issued by any Supervisory Authority.

21. MISCELLANEOUS PROVISIONS

21.1 This DPA and any information disclosed to the Supplier by the Client in relation to the same is confidential and the Supplier will not divulge or disclose it to any Third Party without prior express consent in writing from the Client.

21.2 The Supplier shall not use or permit the use of any IPR belonging to the Client or any of its Affiliates for any purpose whatsoever, without the express prior written consent of the Client.

21.3 The Supplier shall at all times comply with and shall procure that its Personnel comply with the Anti-Bribery & Corruption Policy and all anti-bribery and anti-corruption measures required by Applicable Law.

21.4 This DPA constitutes the entire agreement of the Parties relating to the Processing of Protected Data, to the exclusion of all other terms and conditions, and any prior written or oral agreement between them.

21.5 The Supplier shall not assign, novate, or otherwise transfer all or any of its rights, benefits or obligations under this DPA without the prior written approval of the Client.

21.6 The Supplier shall not sub-contract the performance of any of its obligations under this DPA without the prior written approval of the Client.

21.7 No variation of this DPA shall be effective unless in writing and signed by or on behalf of each Party's Authorised Representative.

21.8 No failure to exercise, nor any delay in exercising, any right, power or remedy under this DPA shall operate or be deemed a waiver of the same. Waivers must always be given in writing.

21.9 If any provision of this DPA is determined to be invalid, illegal or void by any court or administrative body of competent jurisdiction then the rest of this DPA shall still remain in full force and effect.

21.10 Nothing in this DPA shall be construed to make either Party an agent, employee, franchisee, joint venturer or legal representative of the other Party.

21.11 Except where expressly contemplated, this DPA does not create any rights which are enforceable by any Person who is not a Party to this DPA.

21.12 Any notice or other communication given under or in connection with this DPA shall be in writing and shall be delivered by any of the following:

21.12.1 hand to the Party due to receive it at the Party's address;

21.12.2 email to the Party due to receive it at the Party's email address; or

21.12.3 fax to the Party due to receive it at the Party's fax number.

21.13 This DPA is drawn up in the English language and the English language version of this DPA shall always prevail over any translation. This DPA shall be construed, interpreted and administered in English.

21.14 Unless otherwise stated, the rights and remedies of a Party under this DPA are cumulative and do not exclude any other right or remedy provided by Applicable Law.

21.15 This DPA is governed by, and shall be construed in accordance with, the laws of [●].

21.16 The Parties irrevocably submit to the [non /exclusive] jurisdiction of the courts of [●] in relation to any disputes.

EXECUTION

EXECUTED as an Agreement on the date and year first written above.

Signed for and on behalf of
[Insert Company Name and Number]
as its duly authorised representative:

Signature of witness	Signature of duly authorised representative
Name of witness (print)	Name of duly authorised representative (print)

Signed for and on behalf of
[Insert Company Name and Number]
as its duly authorised representative:

Signature of witness	Signature of duly authorised representative
Name of witness (print)	Name of duly authorised representative (print)

SCHEDULE 1 | DEFINITIONS

1. DEFINITIONS

1.1 In this DPA (unless the context otherwise requires), the defined terms shall have the meanings set out below:

Affiliate means any entity that is Controlled by a Party or under common Control of that Party;

Anti-Bribery & Corruption Policy means the anti-bribery and corruption policy of the Client as may be communicated to the Supplier and amended from time to time by the Client;

Applicable Law means all national, state, local and municipal legislation, regulations, statutes, by-laws, Approvals and/or other laws and any other instrument or direction from officials having the force of law as may be issued and in force from time to time (and any amendment or subordinate provisions thereto) relating to or connected with the activities contemplated under this DPA, wherever so located and/or performed;

Approvals means any licenses, permits, consents, approvals and authorisations (statutory, regulatory or otherwise) that a Party may require (whether to comply with Applicable Law or otherwise) to perform its obligations under this DPA;

Audit means an examination of the Audit Items of the Supplier in order to confirm the Processor's compliance with its obligations under or in connection with this DPA;

Audit Items means any books, systems, reports, practices, data, records and documents in the possession, custody or control of the Supplier relating to the Supplier's performance of its obligations under or in connection with this DPA;

Auditor means an auditor appointed by the Client from time to time in order to exercise its rights of Audit under or in connection with this DPA;

Authorised Representative means the duly authorised representative(s) of the Parties for the purpose of entering into and/or varying the terms and conditions of this DPA;

Business Day means a day other than a weekend, official public holiday or a day upon which banks are otherwise generally closed for business in the Territory;

Contract Year means a period of 1 year commencing from the DPA Date, and each additional 1-year period thereafter during the Term;

Control means the:

(1) ownership or control (whether directly or indirectly) of more than 50% of the voting share capital of the relevant entity;

(2) ability to direct the casting of more than 50% of the votes exercisable at general meetings of the relevant entity on all, or substantially all, matters; or

(3) right to appoint or remove directors of the relevant entity holding a majority of the voting rights at meetings of the board on all, or substantially all, matters,

and the terms "Controls", "Controlled" and "Controlling" shall have the equivalent grammatical meaning;

Data Controller means the Person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data;

Data Processor means a Person, public authority, agency or other body which Processes Personal Data on behalf of the Data Controller;

Data Protection Impact Assessment means an assessment by the Data Controller of the impact of the envisaged Processing on the protection of Personal Data;

Data Protection Laws means any Applicable Law relating to the Processing, privacy, storage, destruction, retention and use of Personal Data, as applicable to the Client, the Supplier and/or the services provided by the Supplier;

Data Protection Losses means all liabilities and other amounts, including all: (a) costs (including legal costs), claims, demands, actions, settlements, interest, charges, procedures, expenses, losses and damages; (b) to the extent permitted by Applicable Law: (i) administrative fines, penalties, sanctions, liabilities or other remedies imposed by a Supervisory Authority; (ii) compensation paid to a Data Subject; (iii) costs of compliance with investigations by a Supervisory Authority; and (iv) any loss of or corruption to the data of Clients of the Client;

Data Subject means the natural person to whom Personal Data relates;

Data Subject Request means a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Laws to access their Personal Data;

DPA means this data processing agreement;

DPA Date means the date stated at the top of page 4 of this DPA;

International Recipient means any country outside [the Territory] or any international organisation;

IPR means patents, inventions (whether patentable or not), copyrights, moral rights, design rights, trade-marks, trade names, business names, service marks, brands, logos, service names, trade secrets, know-how, domain names, database rights and any other intellectual property or proprietary rights (whether registered or unregistered, and whether in electronic form or otherwise) including rights in computer software, and all registrations and applications to register any of the aforesaid items, rights in the nature of the aforesaid items in any country or jurisdiction, any rights in the nature of unfair competition rights, and rights to sue for passing off;

Material Breach means:

(1) a breach of this DPA that is not remedied by the breaching Party within 30 days of being notified of the breach;

(2) a persistent pattern of minor breaches of this DPA, which when taken as a whole, constitute a material breach; or

(3) any breach of any term in this DPA which is designated as a Material Breach term;

Person means any natural person, corporate or unincorporated body (whether or not having separate legal personality), individual, corporation, partnership, limited liability company or similar entity;

Personal Data means any information relating to an identified or identifiable natural person, and an “identifiable natural person” is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

Personnel means all employees, agents and Subcontractors of a Party who are assigned, engaged or otherwise employed from time to time to work in connection with the performance or discharge of a Party’s obligations under this DPA;

Processing means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction, and the word “Process” shall have an equivalent grammatical meaning;

Processing Instructions means the written instructions from the Client to the Supplier as to the Processing that is permitted to be carried out to the Protected Data, which as of the DPA Date being as set out in **Schedule 2 (Essential Processing Particulars)** and as communicated by the Client to the Supplier from time to time;

Project means [reference the main agreement which governs the relationship between the parties in connection with the Project];

OR

means [describe the relationship between the Parties for which the Processing of Protected Data is going to occur]

Protected Data means Personal Data received from or on behalf of the Client, or otherwise obtained in connection with the performance of the Supplier’s obligations [under this DPA / in connection with the Project];

Protective Measures means appropriate technical and organisational measures as may be required by Data Protection Laws and Good Industry Practice, which may include:

(1) pseudonymising and encrypting Personal Data,

(2) ensuring confidentiality, integrity, availability and resilience of systems and services;

(3) ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident; and

(4) regularly assessing and evaluating the effectiveness of any such measures adopted by it, including those set out in **Schedule 3 (Security Measures)**;

Subcontractor means any Person subcontracted by a Party to perform or assist in the performance of that Party’s obligations under this DPA;

Sub-processor means any Third Party appointed to Process Protected Data on behalf of the Supplier;

Supervisory Authority means any local, national or multinational agency, department, official, parliament, public or statutory person or any government or professional body, regulatory or supervisory authority, board or other body responsible for administering Data Protection Laws;

Term means the period of [●] months from the DPA Date;

Territory means [●];

Third Party means any Person subcontracted by a Party to perform or assist in the performance of that Party's obligations under this DPA; and

Unauthorised Data Event means any breach of security (regardless of the cause) leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise Processed.

SCHEDULE 2 | ESSENTIAL PROCESSING PARTICULARS

1. REQUIRED PROCESSING

DESCRIPTION	DETAILS
Identity of the Data Controller and Data Processor:	**User note:** Will need to be tweaked if the roles of Data Controller and Data Processor are not clearly defined.
Subject matter of the Processing:	**User note:** Insert high level description of what the Processing is about, e.g. (where Supplier is performing delivery services) Processing required so that Supplier can perform the relevant delivery services to clients of the Client.
Duration of the Processing:	**User note:** Clearly set out the duration of the Processing, including dates
Nature and Purposes of the Processing	**User note:** Please be as specific as possible. • **Examples of "nature"** – collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available alignment or combination, restriction, erasure or destruction of data (whether or not by automated means) etc • **Examples of "purpose"** – employment processing, statutory obligation, recruitment assessment etc.
Type of Protected Data being Processed	**User note: Examples** – name, address, date of birth, telephone number, salary, images, biometric data etc.
Categories of Data Subject	**User note: Examples** – Staff (including volunteers, agents and temporary workers), Clients/clients, suppliers, patients, students/pupils, members of the public, users of a particular website etc.
Plan for return and destruction of the data once the Processing is complete	**User note:** Describe how long the data will be retained for, how it will be returned or destroyed. Note also that this item may not be applicable, if there are union or member state laws to preserve data.

2. PROCESSING INSTRUCTIONS

2.1 [DN: Please set out in detail instructions relating to the Processing of Protected Data.]

SCHEDULE 3 | SECURITY MEASURES

1. SECURITY MEASURES

[DN: Please consider what security measures are appropriate in relation to the type of Protected Data being Processed. Some examples of measures include:

1. External Certifications, e.g. Essential Plus certification, ISO 27001:20134 certification etc
2. Risk Assessment
3. Security Classification of Information
4. End User Device Requirements
5. Testing, e.g. Supplier must procure performance of an ITHC or Penetration Test
6. Networking, e.g. encryption of information transmitted
7. Personnel Security, e.g. pre-employment checks
8. Identity, Authentication and Access Control
9. Data Destruction/Deletion
10. Audit and Protective Monitoring
11. Location of Authority/Buyer Data
12. Vulnerabilities and Corrective Action
13. Secure Architecture, e.g. designing the service in accordance with NSCS “Cloud Security Principles”.]