Data Processing Addendum

This Data Processing Addendum and Standard Contractual Clauses supplement the agreements between 12d Synergy Pty Ltd and the Customer, governing Customer's use of the 12d Synergy Services (the "**Agreement**"). This DPA is supplemental to and forms an integral part of the Agreement and the term of this DPA will follow the term of the Agreement unless it is terminated otherwise and in accordance with the terms and conditions of this DPA.

1. Definitions

    "**12d Synergy Services**" means the Service and/or Application provided by 12d Synergy in accordance with the Agreement entered into between 12d Synergy Pty Ltd and the Customer;

    Commencement date means the earlier of the date of the Agreement, this Data Processing Addendum or the first use of the Services by the Customer;

    "**Customer**" means the recipient of 12d Synergy Services pursuant to the Agreement (the "**Customer**");

    "**Data Breach**" means any unauthorised access to, or disclosure or use by a third party of, personal information or loss, misuse, damage or destruction by any person of personal information;

    "**EU GDPR**" means the General Data Protection Regulation (EU) 2016/679;

    "**Privacy Laws**" means all applicable data protection and privacy legislation in force from time to time in the European Union, the United Kingdom, the United States and Australia, including the EU GDPR, the UK GDPR, the Data Protection Act 2018; the Privacy and Electronic Communications Directive 2002/58/EC (as updated by Directive 2009/136/EC), the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426), the California Consumer Privacy Act of 2018 and the Privacy Act 1988 (Cth) (including the Australian Privacy Principles in Schedule 1 of that Act) as amended, consolidated or replaced from time to time;

    "**Restricted Transfer**" means a transfer of personal information to a country, a territory or specified sector within a country that is (but for the operation of this Agreement): (i) not recognised as providing an adequate level of protection for personal Information under the Privacy Laws (as applicable to the personal information transfer); and (ii) is not subject to any safeguards or derogations that would permit the transfer of the personal information to the country, territory or sector in accordance with the Privacy Laws (as applicable to the personal information transfer).

    Third Party Hosting Provider" means Microsoft Azure or any other provider of hosting services used by Us in the delivery of 12d Synergy Services, with such hosting being provided in Australia;

    "**UK GDPR**" means the EU GDPR as it forms part of the laws of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 and 2020;

"**We**," "**Us**" or "**Our**" means 12d Synergy Pty Ltd

"**You**" or "**Your**" means the Customer; and

"**Your Data**" means all electronic data or information provided by Customer to 12d Synergy in the course of using the 12d Synergy Services.

1. Each party will comply with all applicable requirements of the Privacy Laws. This Data Processing Addendum is in addition to, and does not relieve, remove or replace, a party's obligations or rights under the Privacy Laws.

2. Each party will have in place appropriate policies and procedures to comply, and ensure that its personnel comply, with their respective obligations under all applicable Privacy Laws.

3. The parties acknowledge that:

    (i)   if We process any personal data on Your behalf when performing Our obligations under the Agreement, You are the controller of the personal data and We are the processor of the personal data for the purposes of the Privacy Laws;

    (ii)   **Schedule A** sets out the scope, nature and purpose of processing by Us, the duration of the processing and the types of personal data and categories of data subject; and

    (iii)   the personal data may be used, processed, transferred or stored outside the European Economic Area and the United Kingdom, or the country where You are located, in order to carry out the 12d Synergy Services and Our other obligations under the Agreement.

4. You will ensure that You have all necessary appropriate consents and notices in place to enable lawful transfer of the personal information to Us for the duration and purposes of the Agreement so that We may lawfully use, process, transfer and store the personal information in accordance with the Agreement on Your behalf.

5. We shall, in relation to any personal information processed in connection with the performance by Us of our obligations under the Agreement:

    (i)   process that personal information only on Your documented written instructions unless We are required otherwise by any applicable laws. Where required to process personal information other than in accordance with your instructions, We shall promptly notify You of this before performing the processing required unless those laws prohibit Us from so notifying You;

    (ii)   to the extent that the required information is reasonably available to Us, and You do not otherwise have access to the required information, We will provide reasonable assistance to You:

    (A) in Your fulfilment of Your obligations to respond to requests for exercising data subject's rights;

    (B) in Your compliance with Your obligations under relevant Privacy Laws, including reasonably allowing for and reasonably contributing to audits and inspections conducted by You or another auditor authorised by You. You shall be responsible for any costs incurred by Us in connection with or as the result of providing such information or assistance;

    (C) at Your written direction, delete or return personal information and copies thereof to You on termination of this Agreement unless required by applicable law to store

the personal information (and for these purposes the term "delete" shall mean to put such personal data beyond use or recognition); and

(D) take reasonable steps to ensure that persons authorised by Us (if any) to process the personal information have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

6.   In the event of a Data Breach, We shall:

(i)   notify You without undue delay upon becoming aware of the Data Breach;

(ii)   take reasonable steps to mitigate the effects of and to minimise any damage resulting from the Data Breach; and

(iii) provide reasonable assistance to You in relation to any Data Breach notifications You are required to make under the Privacy Laws.

7.   The following apply to any Restricted Transfers of personal information from You, as controller, to Us, as processor:

(i)   Where that Restricted Transfer is subject to the EU GDPR, Module 2 of the Standard Contractual Clauses ("**SCCs**") for Controller to Processor transfers and Schedule B to this DPA shall apply to any such transfers;

(ii)   Where that Restricted Transfer is subject to the UK GDPR, the parties will use Module 2 of the SCCs together with the UK Addendum to the Standard Contractual Clauses for Controller to Processor transfers and Schedule C to this DPA shall apply to any such transfers

8.   We shall maintain a list of sub-processors and shall notify You of any intended changes concerning the addition or replacement of sub-processors, thereby giving You the opportunity to object to such changes. Any objection to an intended change concerning sub- processors must be accompanied by reasonable and specific grounds and provided to Us in writing within 14 days of receipt of notification of the intended change.

This addendum is executed on behalf of 12dSynergy by its duly authorised signatory, who represents that he/she has the authority in that regard, on the date included below. The Customer accepts the terms of this Data Processing Addendum upon execution or other acceptance of the Agreement.

Customer

Signature:	Signed and accepted by Customer signing and accepting the Agreement
Date:	Dated the date of the Agreement
Role (controller/processor):	**Data Exporter/Controller**

12dSynergy

Signature:	Richard Stoliar 22nd August 2025
Role (controller/processor):	**Processor**

SCHEDULE A

Description of processing

Scope, nature and purpose of processing	We shall process the personal information for the purposes of providing the 12d Synergy Services as set out in the Agreement.
Duration of the processing	For the duration of the Agreement.
Types of personal data	In each case applicable to the 12d Synergy Services: Name, title, work email address for user access and notifications and any other personal information uploaded to the 12d Synergy Services by the Customer, including the personal information of any customers, clients, business partners and suppliers of the Customer.
Categories of data subject	In each case as applicable to the Customer and its use of 12d Synergy Services: • Your employees, contractors and workers. • Your customers, clients, business partners and suppliers.

ANNEXURE I – SCHEDULE A

A. List of parties

Date Exporter	Customer
Name:	As specified in the Agreement
Address:	As specified in the Agreement
Contact person name:	As specified in the Agreement
Position:	As specified in the Agreement
Contact details	As specified in the Agreement

Date Importer	12dSynergy Pty Ltd
Name:	**12d Synergy Pty Ltd** ABN 92 624 225 421
Address:	PO Box 241 Frenchs Forest NSW 1640 Australia
Position:	Privacy Officer
Contact details	Email: privacy@12dsynergy.com Telephone: +61 2 9055 4636

B. Description of transfer

Categories of data subjects whose personal data is transferred	In each case as applicable to the Services: • The Data Exporter's employees, contractors and workers; and • The Data Exporter's customers, clients, business partners and suppliers.
Categories of personal data transferred	In each case as applicable to the Services: • Name, title, work email address for user access and notifications • Any other personal information uploaded to the 12d Synergy Services by the Data Exporter, or otherwise disclosed to the Data

	Importer by the Data Exporter from time to time including the personal information of any customers, clients, business partners and suppliers of the Data Exporter.
Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.	Not applicable. No sensitive data is transferred as part of the Services.
The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).	Data will be transferred on a continuous basis, as applicable to the Services.

Nature of the processing

We shall process the Personal Information for the purposes of providing the Services as set out in the Agreement.

Data Subjects whose Personal Data will be Processed, and applicable markets	Personal Data attributes	Source	Responsibility	Purpose/s
The Data Exporter's employees, contractors and workers. The Data Exporter's customers, clients, business partners and suppliers	Personal data needed to provide and enhance the Services including name, title, work email address for user access and notifications	The Data Exporter	The Data Exporter	To provide and enhance the Services in accordance with the Agreement

	Personal data uploaded to the Services including personal information of any customers, clients, business partners and suppliers of the Data Exporter.			

Purpose(s) of the data transfer and further processing

We shall process the Personal Information for the purposes of providing and enhancing 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

For the duration of the Agreement and for a reasonable period thereafter, in accordance with the Data Importer's Retention Policy and as required by applicable laws.

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

Sub-Processor	Subject matter	Nature of processing	Duration
Microsoft

Hubspot

Xero

AEC Digital Services OPC

Atlassian

Reveal

FreshWorks

SendSafely

Digital Enginuiti

12d UK

Harvest | Personal data needed to provide and enhance the Services including name, title, work email address for user access and notifications

Personal data uploaded to the Services including personal information of any customers, clients, business partners and suppliers of the Data Exporter. | Hosting and data processing services to support the provision and enhancement of the Services or software development services

Business process outsourcing to support the development, maintenance and enhancement of the Services | For the Term |

C.   COMPETENT SUPERVISORY AUTHORITY

The competent supervisory authority in the jurisdiction of incorporation of the Data Exporter.

ANNEXURE II – SCHEDULE A

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

Data Importer must develop, implement, maintain and test adequate technical and organisational measures to protect the confidentiality, integrity, and availability of Customer Data that are no less rigorous than accepted industry practices. The measures below should be implemented as a minimum.

1. SECURITY GOVERNANCE AND COMPLIANCE

a) The Data Importer must maintain and implement an information security management system which documents the Data Importer's organisational structure, the security policies, responsibilities, practices, procedures, processes and resources, used by the Data Importer to manage information security in respect of the provision of the Services, including in relation to the accessing and processing of Customer Data.

b) The Data Importer must ensure that at all times it maintains sufficient resources, management structures and management oversight to allow it to meet its security obligations under this agreement.

c) The Data Importer must establish and use auditable, repeatable and integrated processes to effectively identify, manage and report risks in a manner that is consistent with the nature and scope of the Services.

2. DATA PROTECTION

a) Data Importer shall, at its own expense, protect the confidentiality, authenticity and integrity of Customer Data at rest as well as in transit processed within the infrastructure of the Data Importer or sub-contractors (including sub-processors) Data Importer has engaged to provide services under the Agreement.

b) Customer Data must be encrypted while transmitted over external networks using TLS 1.2 or above. Encryption algorithms and technologies in use shall be publicly validated and subject to the acceptable industry standards (e.g., AES, RSA).

3. DATA AVAILABILITY

a) Data Importer must ensure that a back-up of all relevant Customer Data is made immediately prior to any modification, update, upgrade or other change to its system or the Services that may affect any Customer Data.

b) Data Importer shall implement controls to counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.

c) Data Importer must regularly test (at least annually) and update business continuity and disaster recovery plans to ensure that they are up to date and effective. Upon request from Customer, Data Importer must provide copies of the documentation to demonstrate compliance with the requirements of this clause.

4. DATA ACCESS

a) Data Importer must maintain controls to prevent unauthorized access to systems, networks,

applications and data (including Customer Data). As a minimum, Data Importer shall maintain access management practices that ensure:

    i)   access is granted through an access profile (role);

    ii)   access rights are assigned to a role on a need-to-know basis and least privilege basis to ensure segregation of duties and the assignment of roles follows a structured and documented procedure;

    iii)   users have a unique identifier for their own use so that activities can be traced to the responsible individual;

    iv)   withdrawal of access to Customer Data and related assets is performed in a timely manner for personnel who exit Data Importer's organization or are re-assigned outside the scope of services under the Agreement;

    v)   user accounts and system privileges are regularly reviewed;

    vi)   the use of strong passwords according to industry standards on all systems processing or storing Customer Data;

    vii)   remote access to systems uses multi-factor authentication, and is only provided on a needs basis.

b)   In relation to any access to or use of any part of the Data Exporter's system or infrastructure, the Data Importer must comply with the Data Exporter's s security policies and practices as current from time to time and notified to the Data Importer.

5.   DATA HANDLING

a)   Data Importer must ensure that any Data Exporter Data that it processes is classified and managed in accordance with applicable information classification and data management standards.

b)   Data Importer must ensure that all personnel delivering Services to Data Exporter are made aware of and trained on information security threats and are equipped to support organizational information security policies in general as well as within their specific job functions.

c)   Data Importer must maintain disciplinary procedures to sanction individual unintentional or intentional misconduct leading to a breach of information security policies and procedures.

d)   Upon termination, Data Importer must return in the file format(s) reasonably required by Data Exporter or securely destroy any Data Exporter's Data and Confidential Information provided as part of the Agreement, unless otherwise required to be retained by applicable law.

e)   Data Importer will provide Data Exporter with a list of all sub-contractors engaged to perform services in scope of this Agreement and will notify and seek written permission before engaging a third party to process Data Exporter Data on their behalf.

f)   Data Importer will provide Data Exporter with a list of jurisdictions where Data Exporter data is handled and will notify and seek written permission before handling Data Exporter Data outside the agreed jurisdictions.

6.   PHYSICAL SECURITY

a)   Data Importer must maintain effective procedures to prevent unauthorized physical access, damage and interference to processing facilities, systems, networks and information, including Data Exporter Data, used in delivery of Services, including but not limited to:

i) procedures to monitor physical access to ensure that only authorized personnel are allowed access;

ii) controls to prevent unauthorized removal of Data Exporter Data related to the Services on portable storage media by their personnel.

7. VULNERABILITIES MANAGEMENT & CHANGE MANAGEMENT

a) Data Importer shall implement appropriate change management and capacity management processes, including reviewing and testing all changes before they are deployed in a live environment to ensure that it maintains secure operations of information processing systems.

b) Data Importer must ensure that security is included in development and support processes to maintain the security of application system software and information, including by ensuring that segregation of duty is enforced amongst individuals with development responsibilities and production privileges and by implementing adequate procedural controls to prevent the usage of production data in a test environment.

c) The Data Importer must use an appropriate risk assessment framework to measure risk related to technical vulnerabilities in order to define patch severity/criticality level and shall maintain a vulnerability management process that reduces risks resulting from exploitation of vulnerabilities.

d) Data Importer shall obtain timely information about vulnerabilities applicable to systems, applications and networks being used for or connected to the delivery of services under the Agreement and shall evaluate their exposure to such vulnerabilities and take appropriate measures to address the associated risk in a timely manner.

8. RISK ASSESSMENT AND AUDIT

a) Data Importer shall participate in Data Exporter's third party risk management program by regularly answering applicable questionnaires, providing certificates of compliance as applicable or providing results of security testing. Data Importer also agrees to update Data Exporter when a significant change occurs to Data Importer's Information Security Program or security posture.

b) Data Importer must implement processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of Data Exporter Data handling commensurate with the risk involved in performing the Services in scope of the Agreement.

c) Data Exporter shall, observing a notice period of at least 10 days, be entitled to audit Data Importer, within usual business hours, for the purpose of determining whether Data Importer is in compliance with its obligations under the Agreement. Data Importer will provide Data Exporter's audit representatives with information pertaining, or if necessary reasonable access, to its premises, personnel, data, systems, infrastructure, records, controls, processes, and procedures relating to the provisioning of Services in scope of this Agreement

9. SECURITY INCIDENT MANAGEMENT

a) Data Importer must maintain a consistent and effective approach for security incident management, which includes monitoring capabilities and effective procedures to detect and manage in a timely manner events indicating a potential Security Incident.

b) The Data Importer must perform daily monitoring of the critical events in its environment and have the technical capability to detect anomalies and malicious behaviour.

c) Data Importer shall implement reasonable controls in order to restore the availability and access to Data Exporter Data in a timely manner in the event of a Security Incident.

d) Upon becoming aware of a Security Incident related to systems or data relevant for the delivery of Services under the Agreement (including Data Exporter Data), Data Importer must notify Data Exporter without undue delay Data Importer agrees to promptly cooperate with Data Exporter in any investigations or enquiries of the Security Incident by Data Exporter or by a regulatory or law enforcement agency, including through third-party forensics professionals.

e) Data importer must retain, preserve and make available to Data Exporter all relevant records, logs, files, data reporting and other materials required to comply with applicable law, regulation, industry standards or as otherwise reasonably required by Data Exporter.

f) Data Importer acknowledges that Data Exporter will have sole discretion in assessing whether the Security Incident is likely to result in serious harm to any affected individuals and whether any regulator or law enforcement agency should be notified about such Security Incident.

10. SOLUTIONS SECURITY

To the extent the Data Importer is providing a software solution to Data Exporter that requires to be accessed by Data Exporter staff, the Data Importer must ensure that:

a) The solution supports Multi-factor Authentication (MFA).

b) The solution provides audit logging and alerting capabilities that can be enabled to monitor user activities and transactions.

c) The solution includes patching of your solution/application as part of the scope of the Agreement.

d) The solution includes Role Based Access Controls that allow separation of duties and permissions for individual users (e.g. Administrators vs. regular users

ANNEXURE III – SCHEDULE A

LIST OF SUB-PROCESSORS

For the purposes of **Clause 9 Use of sub-processors**, the controller has authorised the use of the following list of sub-processors:

1.

Name: Microsoft Inc.
Address: Level 27, 1 Denison Street North Sydney NSW 2060
Position: The Microsoft Chief Privacy Officer or the Data Protection Officer for your region

Contact details: via https://www.microsoft.com/en-au/concern/privacy

Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised):

Sub-Processor	Subject matter	Nature of processing	Duration
Microsoft	Your Data comprising personal data	Hosting services to support the provision of the Services	For the Term

2.

Name: Hubspot, Inc.
Address: 25 First Street, 2nd Floor, Cambridge, MA 02141 USA
Position: Privacy and Data Protection Officer
Contact details: via https://preferences.hubspot.com/privacy

Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised):

Sub-Processor	Subject matter	Nature of processing	Duration
Hubspot	Your Data comprising personal data	Services to support the provision of the Services	For the Term

3.

Name: Xero
Address: Level 3 254-260 Burwood Road, Hawthorne, Victoria, 3122
Contact person name: Claire Knight
Position: GM Legal – Global Privacy

Contact details: via https://central.xero.com/s/article/Privacy-at-Xero

Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised):

Sub-Processor	Subject matter	Nature of processing	Duration
Xero	Your Data comprising personal data	Services to support the provision of the Services	For the Term

4.

Name: AEC Digital Services OPC
Address: Unit 3203B East Tower, Tektite Tower/PSEC, Ortigas, Philippines
Contact person name: Rozano Santos

Contact details: Rozano.Santos@aecdservices.com

Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised):

Sub-Processor	Subject matter	Nature of processing	Duration
AEC Digital Services OPC	Your Data comprising personal data	Business process outsourcing to support the development, maintenance and enhancement of the Services	For the Term

5.

Name: Reveal
Address: 14 avenue de l'Opera, 75001 Paris, France
Contact person name: Mr. Alexandre Sadones
Position: Data Protection Officer (DPO)
Contact details: https://reveal.co/legals/privacy-policy

Sub-Processor	Subject matter	Nature of processing	Duration
Reveal	Your Data comprising personal data	Services to support the provision of the Services	For the Term

6.

Name: Atlassian
Address: Level 6, 341 George Street, Sydney, NSW 2000, Australia
Contact details: privacy@atlassian.com

See: https://www.atlassian.com/trust/privacy/country/europe-and-gdpr

Sub-Processor	Subject matter	Nature of processing	Duration
Atlassian	Your Data comprising personal data	Services to support the provision of the Services	For the Term

7.

Name: FreshWorks
Address: Freshworks Inc., 2950 S. Delaware Street, Suite 201, San Mateo, CA 94403
Position: Data Protection Officer (DPO)
Contact details: dpo@freshworks.com
See: https://www.freshworks.com/gdpr/

Sub-Processor	Subject matter	Nature of processing	Duration
FreshWorks	Your Data comprising personal data	Services to support the provision of the Services	For the Term

8.

Name: SendSafely

Contact details: privacy@sendsafely.com
See: https://blog.sendsafely.com/sendsafely-gdpr

Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised):

Sub-Processor	Subject matter	Nature of processing	Duration
SendSafely	Your Data comprising personal data	Services to support the provision of the Services	For the Term

9.

Name: Digital Enginuiti
Contact person name: Privacy Officer

Contact details: privacy@digitalenginuiti.com

Description of processing

Sub-Processor	Subject matter	Nature of processing	Duration
Digital Enginuiti Pty Ltd	Your Data comprising personal data	Business process outsourcing to support the development, maintenance and enhancement of the Services	For the Term

10.
  Name: 12d UK
  Contact person name: Privacy Officer

  Contact details: privacy@12d.co.uk

Description of processing

Sub-Processor	Subject matter	Nature of processing	Duration
12d UK	Your Data comprising personal data	Business process outsourcing to support the development, maintenance and enhancement of the Services	For the Term

11.
  Name: Harvest
  Contact details: See: https://support.getharvest.com/hc/en-us/articles/360048685851-Security-FAQ

Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised):

Sub-Processor	Subject matter	Nature of processing	Duration
Harvest	Your Data comprising personal data	Services to support the provision of the Services	For the Term

12.
  Name: Apollo.io
  Contact details: See: https://www.apollo.io/contact-us

Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised):

Sub-Processor	Subject matter	Nature of processing	Duration
Apollo.io	Your Data comprising personal data	Services to support the provision of the Services	For the Term

ANNEX IV - SUPPLEMENTARY MEASURES FOR INTERNATIONAL DATA TRANSFERS TO ENSURE COMPLIANCE WITH GDPR AND SCHREMS II

Following the recommendations provided by the European Data Protection Board to supplement international data transfers[1] and, in light of the judgement issued by the Court of Justice of the European Union in the Schrems II case[2], the Data Importer shall:

a) enumerate the laws and regulations in the destination country applicable to the importer or its (sub) processors that would permit access by public authorities to the personal data that are subject to the transfer, in particular in the areas of intelligence, law enforcement, administrative and regulatory supervision applicable to the transferred data;

b) in the absence of laws governing the public authorities' access to data, provide information and statistics based on the importer's experience or reports from various sources (e.g. partners, open sources, national case law and decisions from oversight bodies) on access by public authorities to personal data in situations of the kind of the data transfer at hand (i.e. in the specific regulatory area; regarding the type of entities to which the data importer belongs, etc.);

c) indicate which measures are taken to prevent the access to transferred data (if any);

d) provide sufficiently detailed information on all requests of access to personal data by public authorities which the importer has received over a specified period of time, and about the requests received, the data requested, the requesting body and the legal basis for disclosure and to what extent the importer has disclosed the data request;

e) specify whether and to what extent the importer is legally prohibited to provide the information mentioned above.

f) commit to reviewing, under the law of the country of destination, the legality of any order to disclose data, notably whether it remains within the powers granted to the requesting public authority, and to challenge the order if, after a careful assessment, it concludes that there are grounds under the law of the country of destination to do so. When challenging an order, the data importer should seek interim measures to suspend the effects of the order until the court has decided on the merits

g) not disclose the personal data requested until required to do so under the applicable procedural rules

h) commit to providing the minimum amount of information permissible when responding to the order, based on a reasonable interpretation of the order.

i) notify promptly the data subject of the request or order received from the public authorities of the third countries, or of the importer's inability to comply with the contractual commitments

j) assist the data subject in exercising their rights in the third country jurisdiction through ad hoc redress mechanisms and legal counselling

k) adopt and regularly review its internal policies to assess the suitability of the implemented complementary measures and identify and implement additional or alternative solutions, when necessary, to ensure that an essentially equivalent level of protection to that guaranteed within the EEA of the personal data transferred is maintained.

---

[1] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data Version 2.0 Adopted on 18 June 2021.

[2] CJEU judgment of 16 July 2020, Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems

SCHEDULE B

EU Standard Contractual Clauses

If You are situated in the EEA, Module 2 of the Standard Contractual Clauses (the Standard Contractual Clauses) shall apply in relation to the transfer of Personal Data from the EEA, and shall form part of the Agreement, completed as follows:

1. Clause 7 of the Standard Contractual Clauses (Docking Clause) does apply.
2. Clause 9(a) Option 2 (General written authorisation) is selected, and the time period to be specified is 30 days.
3. The option in Clause 11(a) of the Standard Contractual Clauses (Independent dispute resolution body) does not apply.
4. With regard to Clause 17 of the Standard Contractual Clauses (Governing law), the Parties agree that option one shall apply. The Parties agree that the governing law shall be the law of the Republic of Ireland.
5. In Clause 18 of the Standard Contractual Clauses (Choice of forum and jurisdiction), the Parties submit themselves to the jurisdiction of the courts of the Republic of Ireland.
6. Annexure I of the Standard Contractual Clauses shall be deemed agreed and completed with the information set out in Annexure I - Schedule A.
7. Annexure II of the Standard Contractual Clauses shall be deemed agreed and completed with the information set out in Annexure II to Schedule A.
8. Annexure III of the Standard Contractual Clauses shall be deemed agreed and completed with the information set out in Annexure III to Schedule A.

SCHEDULE C

UK Approved Addendum

to EU Standard Contractual Clauses

If You are situated in the United Kingdom, Module 2 of the Standard Contractual Clauses shall apply together with the UK Addendum to the Standard Contractual Clauses (SCCs) in relation to the transfer of Personal Data from the United Kingdom, subject to the following:

Part 1

Table 1: Parties

Start date	Commencement Date	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	See Annex I – Schedule A	See Annex I – Schedule A
Key Contact	See Annex I – Schedule A	See Annex I – Schedule A

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						
2	X	Applies	Option does not apply	Option 2 – General Authorisation	30 days	
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: See Annex I.A – Schedule A
Annex 1B: Description of Transfer: See Annex I.B – Schedule A
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: See Annex II – Schedule A
Annex III: List of Sub processors (Modules 2 and 3 only): See Annex III – Schedule A
Annex IV: Supplementary Measures for International Data Transfers to Ensure Compliance with GDPR and SCHREMS II: See Annex IV– Schedule A

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 **Error! Reference source not found.**: ☒ Importer ☐ Exporter ☐ neither Party

Part 2: Mandatory Clauses

The Alternative Part 2 Mandatory Clauses shall apply, as follows:

Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the Information Commission Office (ICO) and laid before the UK Parliament in accordance with s119A of the Data Protection Act 2018 on 28 January 2022, as it is revised under Section 18 of those mandatory clauses.