APPENDIX 3 – DATA PROCESSING AGREEMENT

ENTERPRISE IRELAND LIMITED

and

[INSERT SUPPLIER NAME]

DATA PROCESSING AGREEMENT

THIS DATA PROCESSING AGREEMENT is made on **[insert date]**

BETWEEN:

(1) **ENTERPRISE IRELAND** with Principal Office at The Plaza, Eastpoint Business Park, Dublin 3 (**EI**); and

(2) [·] (**the Supplier**).
(each a **Party** and together the **Parties**).

BACKGROUND:

(A) The Supplier is [insert description of the Supplier's business activities].

(B) [The Supplier is providing the Services to EI [pursuant to an agreement for [insert type of services e.g. payroll] dated [insert date of agreement] (the **Services Agreement**) [1]].

(C) In the course of providing the Services to EI pursuant to [this Agreement/ the Services Agreement], the Supplier will process Personal Data on behalf of EI. The Supplier agrees to comply with the following provisions with respect to any Personal Data processed on behalf of EI.

AGREED TERMS:

1 DEFINITIONS AND INTERPRETATION

1.1 In this Agreement the following expressions will have the following meanings unless expressly stated to the contrary:

Commencement Date means [·];

Confidential Information means any information, that relates to the business, affairs, operations, customers, processes, budgets, pricing policies, product information, strategies, developments, trade secrets, know-how, methods, technology, technical data,

[1] **Note:** this agreement can be used as a standalone processing agreement (to be included as an appendix to a services agreement). Alternatively, the clauses at sections 2 and 3 can be extracted and included directly in the contract for services with the supplier/data processor. We can assist with this as and when required.

personnel and suppliers of the disclosing party, and any other information clearly designated by a Party as being confidential to it (whether or not it is marked "confidential"), or which ought reasonably be considered to be confidential, or other matters connected with the Services;

Controller Data means all Personal Data and Confidential Information that may be supplied to the Processor by or on behalf of the Controller pursuant to [this Agreement/ the Services Agreement] or produced or obtained by the Processor wholly or partly at the Controller's expense;

Data Controller, **Data Processor**, **Data Subject**, **Personal Data**, **Processing** and **Prior Consultation** shall have the meanings ascribed to them under Data Protection Law;

Data Processing Annex means Annex 1 to this Agreement; ;

Data Protection Law means (i) Data Protection Acts 1988 to 2018 in Ireland (as amended or replaced); (ii) to the extent applicable, the data protection and information privacy laws of another jurisdiction;(iii) the General Data Protection Regulation (EU) 2016/679 (**GDPR**); (iv) any subsequent re-enactment, replacement or amendment of such laws; and (v) any guidance issued by the Irish Data Protection Commission (or replacement Irish supervisory authority);

Data Security Breach means any known potential or actual breach of the Data Controller's minimum information security requirements or any obligations or duties owed by the Data Processor to the Data Controller relating to the confidentiality, integrity or availability of Confidential Information or Personal Data;

Group means of a party means in relation to a party, that party, any subsidiary or holding company of that party, and any subsidiary of a holding company of that party, 'holding company' and 'subsidiary' having the meanings given to them in sections 7 and 8 of the Companies Act 2014 (Ireland);

Losses means all direct, indirect or economic loss (including loss of profits), liability, damage, injury, claim, action, demand, expense (including legal and other professional services expenses on a full indemnity basis) or proceedings awarded against, suffered, incurred or paid by the Controller;

Personnel means (i) the officers, employees, agents and contractors (including

Subcontractors) of a Party and the members of its Group; and (ii) the officers, employees, contractors and agents of the contractors (including Subcontractors) of that Party and the members of its Group;

Regulator means any regulator or regulatory body (including the Office of the Data Protection Commissioner and its successor) to which the Data Controller is subject from time to time or whose consent, approval or authority is required so that the Data Controller can lawfully carry on its business; and

Services mean the services to be delivered by or on behalf of the Data Processor under [this Agreement/ the Services Agreement].

2 DATA CONTROLLER AND DATA PROCESSOR

2.1 In order to provide the Services to EI, the Supplier will require certain Personal Data to be made available to it by EI.

2.2 The Parties acknowledge that for the purposes of Data Protection Law, EI is a Data Controller (the **Controller**) under [this Agreement/ the Services Agreement].

2.3 The Supplier is a Data Processor (the **Processor**) in respect of the Personal Data processed under [this Agreement/ the Services Agreement] on behalf of the Controller. All right, title and interest in the Personal Data shall vest solely in the Controller and the Processor shall not acquire any rights in the Personal Data, except as may be set out in this Agreement [or the Services Agreement].

2.4 The rights and obligations of each party in connection with data processing activities are set out in clause 3 below.

3 DATA PROTECTION OBLIGATIONS

Obligations of the Controller

3.1 The Controller shall provide the Personal Data to the Processor together with such other information as the Processor may reasonably require in order for the Processor to provide the Services to the Controller.

Obligations of the Processor

3.2 **Instructions**: The Processor shall only, and shall procure that its Personnel only, Process the Personal Data to the extent necessary to perform its obligations in accordance with this Agreement, [the Services Agreement] and any other written instructions of the Controller, including those set out in the **Data Processing Annex**, unless required to do so by Union

or Member State law to which the Processor is subject and in such a case, the Processor shall inform the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

3.3 **Disclosure to Third Parties**: The Processor shall not disclose the Controller Data to any third party without the prior written approval of the Controller.

3.4 **Data Transfers**: The Processor shall not transfer any of the Personal Data or other information relating to customers of the Controller to a country outside of the European Economic Area without the correct transfer mechanisms and in accordance with any terms the Controller may impose on such transfer.

3.5 **Data Subject Rights**: The Processor agrees to assist the Controller in responding to requests by Data Subjects exercising their rights under Data Protection Law, within such timescales as may be specified by the Controller.

3.6 **Assistance**: The Processor shall assist the Controller within timescales that allow the Controller to comply with its obligations pursuant to:

Article 32 of the GDPR (Security);

Articles 33 and 34 of the GDPR (Data Breach Notification);

Article 35 of the GDPR (the conduct of Data Protection Impact Assessments); and

Article 36 of the GDPR (Prior Consultation requests to Regulators in relation to Personal Data Processing under this Agreement [or the Services Agreement]).

3.7 **Breach Notification**: The Processor will notify the Controller within twenty-four (24) hours of the Processor becoming aware of a Data Security Breach, and shall include in such notification, at least the applicable information referred to in Article 33(3) of the GDPR. The Processor shall not communicate with any Data Subject in respect of a Data Security Breach without the prior written consent of the Controller.

3.8 **Restoration**: In the event that any of the Controller Data is corrupted or lost or sufficiently degraded as a result of the any negligence or default by the Processor or its Personnel so as to be unusable then, the Controller shall have the option to:

require the Processor at its own expense to use best endeavours to restore or procure the restoration of the Controller Data and the Processor shall use best endeavours to do so as soon as possible; or

itself restore or procure the restoration of the Controller Data and require the Processor to reimburse the Controller for any costs incurred in so doing.

3.9 **Confidentiality**: The Processor will ensure that its Personnel who Process Personal Data under this Agreement [and the Services Agreement] are subject to obligations of confidentiality in relation to such Personal Data.

3.10 **Security**: The Processor shall implement appropriate technical and organisational measures to assure a level of security appropriate to the risk to the security of Personal Data, in particular, from accidental or unlawful destruction, loss, alteration, unauthorised, disclosure of or access to Personal Data including as appropriate:

the pseudonymisation and encryption of Personal Data;

the ability to ensure the ongoing confidentiality, integrity and availability and resilience of the Processor's systems used for such Processing, the Personal Data and the Services;

the ability to restore the availability and access to the Personal Data in the event of a physical or technical incident; and

a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

3.11 The Processor shall notify the Controller of any material changes to the technical and organisational measures used by the Processor throughout the Term.

3.12 **Sub-Processing**: The Processor agrees that it shall not engage any third party to Process the Controller's Personal Data without the prior written consent of the Controller. The Processor shall inform the Controller of any intended changes concerning the addition or replacement of the other processors and shall not make any such changes without the prior written consent of the Controller.

3.13 If the Processor engages any third party to Process any of the Controller's Personal Data,

the Processor shall impose on such third party, by means of a written contract, the same data protection obligations as set out in this Agreement and shall ensure that if any third party engaged by the Processor in turn engages another person to Process any Personal Data, the third party is required to comply with all of the obligations in respect of Processing of Personal Data that are imposed under this Agreement.

3.14 The Processor shall remain fully liable to the Controller for Processing by any third party as if the Processing was being conducted by the Processor and the limitations on liability agreed in clause.

3.15 **Demonstrating Compliance**: The Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations set out in Article 28 of the GDPR and allow for and contribute to audits, including inspections, conducted by EI or another auditor mandated by EI.

3.16 **Infringement**: The Processor will immediately inform the Controller if, in its opinion, an instruction given or request made pursuant to this Agreement [or the Services Agreement] infringes Data Protection Law.

3.17 **Termination/Expiry**: On termination or expiry of [this Agreement/ the Services Agreement] (or at any other time on request by the Controller), the Processor shall return or permanently erase, at the election of EI, all copies of Personal Data received and/or processed by it under [this Agreement/ the Services Agreement] unless European Union or Member State law requires retention of the Personal Data.

3.18 The provisions of this clause shall survive the Term until the Processor has returned or destroyed all Personal Data.

Processor Indemnity

3.19

a) The Processor agrees to indemnify the Controller against any and all losses, costs, expenses (including legal expenses), damages, liabilities, demands, claims, fines, actions or proceedings which the Controller may suffer or incur arising out of any breach of this Agreement whether or not such losses were foreseeable at the time of the breach which occasioned them.

b) The total aggregate liability of the Processor, in respect of all claims arising from a breach of the Processor's obligations under Data Protection Law(s), including, for the avoidance of doubt, such obligations under the Framework Agreement and under any Call Off Contract made thereunder or under this Agreement entered into between the parties shall be limited to the greater of (i) 200% of the charges paid or payable by the Controller to the Processor over the term of the Framework Agreement, or (ii)

€1,000,000 (one million euro). This liability cap shall also apply to any indemnity from the Processor under clause 3.19 (a) hereof.

c) The Processor shall not be liable to the Controller for any indirect, consequential or special loss, or any loss of profits or loss of revenue arising out of, or in connection with this Agreement. The following types of losses are however agreed to be reasonably foreseeable and constitute direct and recoverable losses under this Agreement to the extent they are a direct result of a breach of this Agreement by the Processor and do not exceed the cap set out in Clause 19 (b):

(i) the reasonable costs of reconstructing or reloading data caused by a breach by the Processor; and

(ii) any official, legal, administrative and/or regulatory fines, penalties or sanctions levied against the Controller or any of its and/or their representatives arising by virtue of any act, error or omission on the part of the Processor.

d) Nothing in this clause 3.19 shall exclude or limit the Processor's:

- liability for death or personal injury caused by its (or its agent's or subcontractor's or their respective employee's) negligence,
- liability for fraud or fraudulent misrepresentation (or that of their agents, Sub-Contractors or respective employees);

4 TERM AND TERMINATION

4.1 This Agreement shall come into force on the Commencement Date and shall, subject to the terms of clauses 3.17, 3.18 and 3.19, terminate on [insert date/ termination or expiry of the Services Agreement**] (the Term).**

5 GENERAL

5.1 **Counterparts**: this Agreement may be executed in any number of counterparts, each of which when executed and delivered shall constitute an original of this Agreement.

5.2 **Governing Law**: The formation, existence, construction, performance, validity and all aspects whatsoever of this Agreement or of any term of this Agreement will be governed by Irish law. The Parties irrevocably agree to submit to the exclusive jurisdiction of the courts of Ireland over any claim or matter arising under or in connection with this Agreement.

5.3 **Severability**: If any provision of this Agreement shall be held to be void or declared illegal, invalid or unenforceable for any reason whatsoever, such provision shall be divisible from this Agreement and shall be deemed to be deleted from this Agreement and the validity of the remaining provisions shall not be affected.

IN WITNESS whereof this Agreement has been duly executed by the parties to it on the date set out at the beginning of this Agreement.

Signed for and on behalf of **Enterprise Ireland**	Signed for and on behalf of the **Supplier**
Signed _____	Signed _____
Duly authorised by **Enterprise Ireland**	Duly authorised by the **Supplier**
Name _____	Name _____
Title _____	Title _____
Date _____	Date _____

ANNEX 1 (TECHNICAL AND ORGANISATIONAL MEASURES/DATA PROCESSING ANNEX)

Data Flows and/or Record of Processing

Please complete a data flow diagram(s) showing the flow of personal data involved in the delivery of the service. The diagram should show **data** inputs, outputs, storage points including any 3rd parties who are involved in processing the data for all components of service delivery.

The Supplier may choose to complete a record of processing activities (ROPA) table to describe the data processing activities. Where supplied, The ROPA should include the information outlined in Article 30.

DATA RECORD

Complete the following Data Record

<table>
<tr><td colspan="2">Customer:</td><td>Supplier:</td></tr>
<tr><td colspan="2">Customer Contact Name:</td><td>Supplier Contact Name:</td></tr>
<tr><td>Nature and purpose of the processing carried out by Supplier:</td><td colspan="2">[Insert a description of the purpose of processing]</td></tr>
<tr><td>Duration of Processing:</td><td colspan="2">[Insert agreed requirements around retention and deletion of the Personal Data]</td></tr>
<tr><td>Description of data subject:</td><td colspan="2">[Insert description of data subject, ie. Employees, members of the public etc.]</td></tr>
<tr><td>Personal Data processed as part of the Services:</td><td colspan="2">Delete data sets which are not applicable and/or add further data sets which are not included in the table.
<table><tr><td>Identification Data</td><td>includes name, date of birth, driver’s license and passport information.</td></tr></table></td></tr>
</table>

Contact Data	includes email address, phone number, postal address, other communication details (e.g. Skype)
Communication Data	includes phone calls, email correspondence and hard copy correspondence.
Marketing Data	includes Contact Data and any preferences in receiving marketing and communication preferences.
Employee Data	Includes HR records, leave data, personal development information (PD), training records, health information
Recruitment Data	includes recruitment related data such as Identification Data, Contact Data, Communication Data, CV and job application data. CV data may include employment history, skills/ experience, languages, educational history, qualifications, membership of professional associations, contact details of employer references/character references, licenses held, interests and hobbies, languages, locations, nationality, passport, eligibility to work in certain jurisdictions, salary expectations, interview/screening answers and notes.
Financial Data	includes payment related information or bank account details and financial data, pension data.
Web Data	includes Personal Data provided on any forms on our website and, to the extent that it includes Personal Data, information on the type of device used, IP address, operating system, referral source, length of visit, page views and website navigation paths, as well as information about the timing, frequency and pattern of service use. Includes cookies, beacons or other tracking or profiling technologies.
Special Category Data	this can include diversity data such as gender, religion, racial or ethnic origin, sexual orientation, trade union membership or data relating to health [include relevant headings as appropriate]

Authorised Sub-Processors and transfers: e.g. webservices, email platforms, customer support, other vendors or software/platforms etc.	**Sub-Processor**	**Services**	**Location**	**Transfer mechanism (if applicable)**
	Microsoft Corporation (Example)	*Email delivery, Azure services*	*EU and US (support)*	*Standard Contractual Clauses*
				Standard Contractual Clauses/ Binding Corporate Rules?
				Standard Contractual Clauses/ Binding Corporate Rules?
				Standard Contractual Clauses /Binding Corporate Rules?
				Standard Contractual Clauses/ Binding Corporate Rules?
Supplier TOMs:	**Technical and Organisational Measures (TOMS) Declaration Below**			

Processor Due Diligence Questions	
Please provide the contact details of the Data Protection Lead/DPO/Privacy Manager	
Please confirm all Supplier staff who will be involved in the processing of personal data on behalf of Enterprise Ireland regularly receive appropriate Data Protection training.	
Please confirm that the supplier has documented an Information Security policy that details appropriate information security measures in relation to the processing of personal data carried out on behalf of Enterprise Ireland.	
Please confirm that the supplier has a Data Protection Policy that details appropriate data protection measures in relation to the processing of personal data carried out on behalf of Enterprise Ireland.	
Please confirm the location(s) where the processing will be carried out.	List Locations Country/City

Please confirm the location(s) where processed data will be stored.	List Locations Country/City
Where processing is carried out outside the EEA or data is stored outside the EEA please indicate which transfer mechanisms are in place to safeguard the data.	
Please indicate if you have any relevant certifications e.g ISO27001/ ISO27701/27017/27018 etc, or if you have undergone any other independent audit of your information security controls, such as SOC2 If yes, please include a copy of the certificate or a link to an online version of the certificate as part of this response, clearly showing the scope of the certification and the certification body. Please also include the Statement of Applicability.	
Please confirm agreement that the following Technical and Organisational Measures have been implemented by the supplier in relation to the processing of personal data carried out on behalf of Enterprise Ireland.	

Please confirm agreement by indicating yes or no to the following TOMs – where no, please provide explanation

TECHNICAL AND ORGANISATIONAL MEASURES		
CONTROL	**REQUIREMENT**	**ACCEPT** **Please indicate Yes/No** **if no, provide details**
Management commitment to Data Protection	Supplier demonstrates commitment to implementing appropriate Technical and Organisational Measures in such a manner that processing of personal data carried out on behalf of Enterprise Ireland meets the requirements of the GDPR and ensures the protection of the privacy rights of data subjects. Supplier has documented data protection policies and there is regular management oversight of the implementation of the policies	

TECHNICAL AND ORGANISATIONAL MEASURES		
CONTROL	**REQUIREMENT**	**ACCEPT** **Please indicate Yes/No** **if no, provide details**
Data Protection Roles and Responsibilities	Supplier has defined clear Data Protection roles and responsibilities in the organisation. The key staff members have received appropriate training and have been allocated the necessary resources to carry out their duties.	
Appointment of a Data Protection Officer (DPO)	Supplier has evaluated the requirement to appoint a Data Protection Officer (DPO). • Where appointed the DPO has been registered with the Data Protection Commission (DPC). • Where a DPO is not required a Data Protection Lead has been identified. The DPO/DP Lead has responsibility for monitoring compliance with the GDPR and with the policies of the organisation in relation to the protection and security of personal data.	
Data Protection Policy and related policy documents	Supplier documents appropriate data protection measures in relation to the processing of personal data carried out on behalf of Enterprise Ireland. The data protection policy addresses Supplier' responsibilities to process personal data in an appropriate and lawful manner, in accordance with DP Laws.	
Awareness & Training	All employees and individual contractors of Supplier involved in processing personal data receive regular appropriate Data Protection and Data Security Training.	
Confidentiality Agreement	All Supplier employees involved in the processing of personal data carried out on behalf of Enterprise Ireland on behalf of Supplier are bound by confidentiality agreements. These agreements include appropriate post-termination clauses.	

TECHNICAL AND ORGANISATIONAL MEASURES		
CONTROL	**REQUIREMENT**	**ACCEPT** **Please indicate Yes/No** **if no, provide details**
Termination of Employment	Access to systems processing personal data on behalf of Enterprise Ireland is revoked immediately on termination of employment.	
Supplier/Partner Management	Supplier incorporates data protection measures into sub-processor activities by: • Implementing Data Processing Agreements (DPAs) that are compliant with Art 28 of the GDPR. • Where relevant, sub-processors are assessed on an ongoing basis to ensure the establishment of adequate safeguards for processing personal data • Specifically, processors are assessed/selected for security of processing and physical storage (location) of personal data. All sub-processing must be carried out under contract. Sub-processor contracts are assessed to ensure adequate safeguards are in place.	
Transferring personal data outside the European Economic Area (EEA)	Where applicable, Supplier has taken measures to meet GDPR requirements for international data transfer of personal data processed.	
Data Security Risk Management	Supplier undertakes an analysis of the risks presented by data processing activities and uses this to ensure the appropriate level of security is put in place.	
Breach Incident Management	Supplier has implemented Breach Management measures including responsibilities and procedures to identify and investigate incidents The supplier policies and procedures include provision for reporting data breach events and security weaknesses that may impact personal data processed on behalf of	

TECHNICAL AND ORGANISATIONAL MEASURES		
CONTROL	**REQUIREMENT**	**ACCEPT** **Please indicate Yes/No** **if no, provide details**
	Enterprise Ireland to Enterprise Ireland without undue delay. Supplier can support incident investigations, in particular through the provision of access to appropriate log data.	
Data Subject Rights Request (DSR) Management	Supplier has documented and implemented DSR measures including a procedure for reporting any DSRs received regarding personal data processed on behalf of Enterprise Ireland and the procedures the processor will follow to support DSR responses received by Enterprise Ireland where applicable.	
Purpose Limitation	Supplier reviews its processing activities regularly to ensure that the processing remains consistent with the purposes for processing outlined in the supplier contracts with Enterprise Ireland.	
Data Minimisation	Supplier ensures that it only processes data that is necessary to carry out the contracted processing on behalf of Enterprise Ireland.	
Privacy by Design	Supplier evaluates the requirement to carry out Data Protection Impact Assessments whenever it is implementing changes to the software and/or services. Where a Data Protection Impact Assessment is carried out Supplier makes summary findings available – particularly where such finding may be necessary to support client DPIAs.	

TECHNICAL AND ORGANISATIONAL MEASURES		
CONTROL	**REQUIREMENT**	**ACCEPT** **Please indicate Yes/No** **if no, provide details**
Information Security governance	Supplier has established, documented, approved, communicated and applied policies and procedures for an information security governance programme, which is sponsored by the leadership of the organisation. Roles and responsibilities for information security are clearly identified and assigned.	
Asset Management	Supplier can identify all information assets relevant to the services provided to Enterprise Ireland and the functions that rely on them.	
Information security measures	Supplier documents appropriate information security measures in relation to the processing of personal data carried out on behalf of Enterprise Ireland. Supplier ensures regular testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. Supplier has implemented security measures to ensure: • only authorised personnel use their computer system • that regular file and e-mail housekeeping, e.g. backups, deleting obsolete files is undertaken • any breaches of policy are reported to a Company Director / IT Manager /Data Protection Officer • staff take appropriate care of all computer equipment assigned to them, e.g. PCs, laptops, Smartphones, printers. • computer equipment (e.g. laptops) is never left unattended in public places or visible in a car.	

TECHNICAL AND ORGANISATIONAL MEASURES		
CONTROL	**REQUIREMENT**	**ACCEPT** **Please indicate Yes/No** **if no, provide details**
Security & Privacy Policies Governance	Mechanisms exist to review security and privacy policies, standards and procedures at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	
Acceptable Usage of Information Systems/Assets	Supplier defines an acceptable use policy to ensure uniform and appropriate use of an organisation's network, computer, information assets, and other electronic resources.	
Access Controls	Supplier has documented and implemented access controls to the Web, Application Servers, Databases and other equipment or information assets containing personal data processed on behalf of Enterprise Ireland. Access controls are implemented based on business requirements. Access to systems is granted on the principle of least privilege and ensures appropriate segregation of duties.	
User Access Management	Supplier has documented and implemented access control and Joiners/Movers/Leavers policies that ensure access to personal data processed on behalf of Enterprise Ireland is authenticated using individual usernames and passwords. Only employees and other parties working on behalf supplier that need access to, and use of, personal data in order to perform their work are provided with access to personal data held by supplier. Domain access is controlled on a role basis. User access is regularly reviewed.	

TECHNICAL AND ORGANISATIONAL MEASURES		
CONTROL	**REQUIREMENT**	**ACCEPT** **Please indicate Yes/No** **if no, provide details**
Two-Factor Authentication	Access to key applications involved in processing of personal data for Enterprise Ireland and in particular to applications that process personal data of a sensitive nature is protected using multi-factor authentication.	
Role-Based Access controls	Access to systems is determined based on individual role-based access and reviewed on a regular basis for continued business need. Access is granted to employees, partners or suppliers according to their role, only to a minimum level that will allow them to carry out their duties, in accordance with the principle of least privilege.	
Password management	Passwords are stored hashed and salted and are never stored or communicated in plaintext.	
Network Security	Supplier implements network security infrastructure such as Firewalls, Intrusion Detection/Prevention Systems (IDS/IPS) and other security controls that provide continuous monitoring, restrict unauthorized network traffic, detect and limit the impact of attacks	
Electronic Communications Security	Supplier communicates guidelines on the appropriate use of email and other communication platforms with all staff and contractors. This includes: • Proper internet usage • Proper use of email, phone, text and social media communications	
Retention and Deletion of data	Supplier has implemented measures to ensure data is only retained for the periods outlined in the contract and to	

TECHNICAL AND ORGANISATIONAL MEASURES		
CONTROL	**REQUIREMENT**	**ACCEPT** **Please indicate Yes/No** **if no, provide details**
	ensure data is securely deleted on contract termination with a mechanism for securely exfiltrating the data if required. Details of secure data deletion can be provided to Enterprise Ireland on request.	
Mobile Device Security	Supplier ensures that it has appropriate authentication and authorisation procedures in place for any Mobile Devices used to process personal data on behalf of Enterprise Ireland (Laptop/Smartphone/Removable Storage) and that personal data processed on behalf of Enterprise Ireland is encrypted and can only be accessed with logon credentials (username/password). Mobile devices must be managed by the Supplier and must be capable of being remotely wiped in the event of loss or theft. Supplier should not permit staff to process personal data on behalf of Enterprise Ireland on personal devices.	
Removable Devices	Supplier ensures that Enterprise Ireland data is never transferred to removeable media.	
Physical Security	Supplier implements physical entry controls to Supplier premises/office building where personal data processed on behalf of Enterprise Ireland is stored or accessed. Where Personal Data is stored in a private or public Cloud, supplier evaluates that the Physical security measures the Cloud Service Provider or hoster has in place are appropriate to the risks to personal data and in particular special category personal data.	

TECHNICAL AND ORGANISATIONAL MEASURES		
CONTROL	**REQUIREMENT**	**ACCEPT** **Please indicate Yes/No** **if no, provide details**
Encryption	Supplier has a documented policy for Cryptography, Encryption and Key Management.	
Encryption In transit	Supplier has implemented measures to ensure that personal data processed is at a minimum encrypted in transit. Deprecated encryption protocols, libraries or ciphers must not be used.	
Encryption at rest	Where applicable, Supplier has implemented measures to ensure that any special categories of personal data processed is always encrypted. • Supplier ensures that all laptops, mobile devices and backup tapes are encrypted in this manner. • Staff who use their own devices to access supplier systems must install authentication software. • Special category data is encrypted within databases. • Deprecated encryption protocols or ciphers must not be used.	
Backups	Supplier has established an appropriate backup process to ensure that it can restore access to personal data in the event of any incidents and to ensure confidentiality, integrity and availability for the personal data that is processed. Regular testing and reviews of our measures are undertaken to ensure they remain effective, and act on the results of those tests where they highlight areas for improvement.	
Business Continuity & Disaster Recovery Policy	Supplier has documented and implemented appropriate Business Continuity & Disaster Recovery measures in relation to the processing of personal data carried out on behalf of Enterprise Ireland.	

TECHNICAL AND ORGANISATIONAL MEASURES		
CONTROL	**REQUIREMENT**	**ACCEPT** **Please indicate Yes/No** **if no, provide details**
	The Business Continuity & Disaster Recovery Plan documents the procedures to be followed to: • handle any unforeseen event that requires disaster recovery • ensure recovery from interruptions is as quick as possible • minimise the impact of interruptions to the systems, to Enterprise Ireland and to the data subjects • support affected Customers in the scenario of a Disaster Recovery situation. Business Continuity Plans (BCP) and Disaster Recovery (DR) Plans must ensure the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident, including data loss or destruction for example by ransomware	
Remote Access Controls	Remote access into Supplier network must be approved and restricted to authorized personnel. Remote access support sessions such as system upgrades or general investigations must be logged by the provider and the logfiles provided to Enterprise Ireland as a record of the session if required. Individual remote access sessions (e.g. to an individuals laptop) must be supervised by the individual.	
Security Audit	Supplier and sub-suppliers carry out Internal and external Security Audits on a regular basis, or whenever a significant infrastructure change is required. Records of all internal and external audits are retained and can be made available to Enterprise Ireland on request.	

TECHNICAL AND ORGANISATIONAL MEASURES		
CONTROL	**REQUIREMENT**	**ACCEPT** **Please indicate Yes/No** **if no, provide details**
Threat and Vulnerability Management	Supplier maintains measures meant to identify, manage, mitigate and/or remediate vulnerabilities within the Supplier and any hosted computing environments. Host and guest operating systems are hardened appropriate to their role. Penetration testing (Internet facing systems) with immediate remediation of identified vulnerabilities. Results of penetration testing to be made available to EI on request.	
Change Management (System Updates)	Supplier maintains policies and procedures designed to manage risks associated with the application of changes to its systems. Prior to implementation, changes to systems, networks and underlying components, will be documented in a registered change request that includes a description and reason for the change, implementation details and schedule, a risk statement addressing impact, expected outcome, rollback plan, and documented approval by authorized personnel.	
Malware controls	Malware controls must be in place on all information systems processing EI data that: (i) Implement and maintain software for that detects, prevents, removes, and remedies software or computer code designed to perform an unauthorized function on, or permit unauthorized access to, an information system, including without limitation, computer viruses, Trojan horses, worms, spyware, and time or logic bombs ("Malicious Code Software"), (ii) Run Malicious Code Software on at least a daily basis,	

TECHNICAL AND ORGANISATIONAL MEASURES		
CONTROL	**REQUIREMENT**	**ACCEPT** **Please indicate Yes/No** **if no, provide details**
	(iii) Update Malicious Code Software on at least a daily basis, including without limitation, obtaining and implementing the most currently available malicious code signatures.	
Intrusion detection and response policies, standards and procedures	Supplier must maintain policies, standards and procedures for detecting, monitoring and responding to actual or reasonably suspected intrusions and Security Breaches, and encouraging reporting actual or reasonably suspected Security Breaches, including; (i) training Supplier's personnel with access to Information to recognize actual or potential Security Breaches and to escalate and notify the senior management of the foregoing, (ii) mandatory post-incident review of events and actions taken concerning security of Information, and (iii) policies and standards concerning reporting to Regulators and law enforcement agencies.	
Secure disposal	Supplier has policies and procedures in place to ensure the secure disposal of equipment that may contain Enterprise Ireland data.	
Log management	Events, alerts and log information is reviewed on a timely basis to identify potential security incidents. Supplier retains relevant logs in a tamper proof system that supports threat identification and post-incident investigation.	

TECHNICAL AND ORGANISATIONAL MEASURES		
CONTROL	**REQUIREMENT**	**ACCEPT** **Please indicate Yes/No** **if no, provide details**
Tenant separation	Supplier must ensure that Enterprise Ireland information is segregated from other tenants and that technical controls are in place to maintain and monitor data and user segregation	
Secure software development	Supplier must have established rules for the secure development of software and systems, incorporating at least the OWASP secure coding practices and security principles. A secure software development policy and lifecycle must be in place so that 1. Rules for the secure development of software and systems are established and applied to developments within the organization, 2. Separation of development, testing and operational environments, including protect secure development environments for system development is in place, 3. Testing of security functionality is carried out during development. Systems and apps must be independently penetration tested against at least the OWASP Top 10 Web Application Security Risks before release.	
PCI DSS **Applies only to Managed/Cloud based Services*	Supplier must be compliant with the Payment Card Industry Data Security Standard (PCI DSS) and have the relevant Attestation of Compliance (AoC) or Report on Compliance (RoC) documentation.	

TECHNICAL AND ORGANISATIONAL MEASURES		
CONTROL	**REQUIREMENT**	**ACCEPT** **Please indicate Yes/No** **if no, provide details**
processing payment card data.		
Cookies & other Tracking Technologies	Supplier's platform must be compliant with ePrivacy Regulations & the GDPR as set out by the Data Protection Commissioners guidance on Cookies & Other tracking technologies i.e., only strictly necessary cookies are dropped without consent, all other cookies require consent.	

Any additional details relevant to the above requirements:
