Polasaithe
Naíonra Céimeanna Beaga

Polasaí 57
: Supplier Data Processing Agreement

Gleann Aibhne,

Br. An Ghoirt,

Inis,

Co. an Chláir.

Stiúrthóir: Katie Uí Chaoimh, Fón: (086) 2114881

r-phost: naionragmc@gmail.com

Suíomh gréasáin: www.gmci.ie/naionra

Version	1.0
Date	Nov 2018
Policy Number	Policy Number 57
Owner	Naíonra Céimeanna Beaga
Validity and document management	This document is valid from Nov 1 2018. The owner of this document is the Owner / Manager, who must check and, if necessary, update the document at least once a year. This policy was adopted by Naíonra Céimeanna Beaga on 1 Nov 2018. Signed by: **Katie Uí Chaoimh;** Príomh Stiúthóir on behalf of Naíonra Céimeanna Beaga

Table of contents

1. Introduction

This Supplier Data Processing Agreement ("**Agreement**"), dated [Date] ("**Agreement Effective Date**") forms part of the [Commercial Agreement Name & Date] "**Principal Agreement**") between:

Naíonra Céimeanna Beaga (hereinafter referred as the "**Controller**") acting on its own behalf;
and
[Supplier Name] (hereinafter referred as the **"Processor**") acting on its own behalf.

The terms used in this Agreement shall have the meanings set forth in this Addendum. Terms not otherwise defined herein shall have the meaning given to them in the Principal Agreement. Except as modified below, the terms of the Principal Agreement shall remain in full force and effect. The parties hereby agree that the terms and conditions set out below shall be added as an Addendum to the Principal Agreement.

2. Definitions

In this Agreement, the following terms shall have the meanings set out below and related terms shall be construed accordingly:

- ***"Authorised Sub-processors"*** means (a) those Sub-processors set out in Annex 3 (Authorised Transfers of Controller Personal Data); and (b) any additional Sub-processors consented to in writing by Controller in accordance with Sub-processing section.
- ***"Sub-processor"*** means any Data Processor (including any third party) appointed by the Processor to process Controller Personal Data on behalf of the Controller.
- ***"Process/Processing/Processed", "Data Controller", "Data Processor", "Data Subject", "Personal Data", "Special Categories of Personal Data"*** and any further definition not included under this Agreement or the Principal Agreement shall have the same meaning as in EU General Data Protection Regulation 2016/679 of the European Parliament and of the Council ("GDPR").
- ***"Data Protection Laws"*** means EU General Data Protection Regulation 2016/679 of the European Parliament and of the Council ("GDPR") as well as any local data protection laws**.**
- ***"Erasure"*** means the removal or destruction of Personal Data such that it cannot be recovered or reconstructed**.**
- ***"EEA"*** means the European Economic Area.
- ***"Third country*****"** means any country outside EU/EEA, except where that country is the subject of a valid adequacy decision by the European Commission on the protection of Personal Data in Third Countries.
- ***"Controller Personal Data"*** means the data described in Annex 1 and any other Personal Data processed by Processor on behalf of the Controller pursuant to or in connection with the Principal Agreement**.**

- ***"Personal Data Breach"*** means a breach of leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Controller Personal Data transmitted, stored or otherwise processed*.*
- ***"Services"*** means the services to be supplied by the Processor to the Controller pursuant to the Principal Agreement*.*
- ***"Products"*** means the products to be supplied by the Processor to the Controller pursuant to the Principal Agreement*.*
- ***"Standard Contractual Clauses"*** means the standard contractual clauses for the transfer of personal data to Processors established in third countries, as approved by the European Commission Decision 2010/87/EU, or any set of clauses approved by the European Commission which amends, replaces or supersedes these.

3. Data Processing Terms

In the course of providing the Services and/or Products to the Controller pursuant to the Principal Agreement, the Processor may process Controller personal data on behalf of the Controller as per the terms of this Addendum. The Processor agrees to comply with the following provisions with respect to any Controller personal data. To the extent required by applicable Data Protection Laws, the Processor shall obtain and maintain all necessary licenses, authorizations and permits necessary to process personal data including personal data mentioned in Annex 1.

The Processor shall maintain all the technical and organisational measures to comply with the requirements set forth in the Addendum and its Annexes.

4. Processing of Controller Personal Data

The Processor shall only process Controller Personal Data for the purposes of the Principal Agreement. The Processor shall not process, transfer, modify, amend or alter the Controller Personal Data or disclose or permit the disclosure of the Controller personal data to any third party other than in accordance with Controller's documented instructions, unless processing is required by EU or Member State law to which Processor is subject. The Processor shall, to the extent permitted by such law, inform the Controller of that legal requirement before processing the Personal Data and comply with the Controller's instructions to minimize, as much as possible, the scope of the disclosure.

For the purposes set out in the section above, the Controller hereby instructs the Processor to transfer Controller Personal Data to the recipients in the Third Countries listed in Annex 3 (Authorised Transfers of Controller Personal Data).

5. Reliability and Non–Disclosure

The Processor shall take reasonable steps to ensure the reliability of any employee, agent or contractor who may have access to the Controller personal data, ensuring in each case that access is strictly limited to those individuals who require access to the relevant Controller Personal Data.

The Processor must ensure that all individuals which have a duty to process controller personal data:

- Are informed of the confidential nature of the Controller Personal Data and are aware of Processor's obligations under this Addendum and the Principal Agreement in relation to the Controller Personal Data;

- Have undertaken appropriate training/certifications in relation to the Data Protection Laws or any other training/certifications requested by Controller;
- Are subject to confidentiality undertakings or professional or statutory obligations of confidentiality; and
- Are subject to user authentication and logon processes when accessing the Controller Personal Data in accordance with this Agreement, the Principal Agreement and the applicable Data Protection Laws.

6. Personal Data Security

Taking into account the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Processor shall implement appropriate technical and organisational measures (Annex 2) to ensure a level of Controller Personal Data security appropriate to the risk, including but not limited to:

- Pseudonymization and encryption;
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- The ability to restore the availability and access to Controller Personal Data in a timely manner in the event of a physical or technical incident; and
- A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the Processing.

In assessing the appropriate level of security, the Processor shall take into account the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Controller Personal Data transmitted, stored or otherwise processed.

7. Sub-Processing

As of the Addendum Effective Date, the Controller hereby authorises the Processor to engage those Sub-Processors set out in Annex 4 (Authorised Sub-Processors). The Processor shall not engage any Data Sub-Processors to Process Controller Personal Data other than with the prior written consent of Controller, which Controller may refuse with absolute discretion.

With respect to each Sub-Processor, the Processor shall:

- Provide the Controller with full details of the Processing to be undertaken by each Sub-processor.
- Carry out adequate due diligence on each Sub-Processor to ensure that it can provide the level of protection for Controller Personal Data, including without limitation, sufficient guarantees to implement appropriate technical and organisational measures in such a manner that Processing will meet the requirements of GDPR, this Agreement, the Principal Agreement and the applicable Data Protection Laws.
- Include terms in the contract between the Processor and each Sub-processor which are the same as those set out in this Addendum. Upon request, the Processor shall provide a copy of its agreements with Sub-Processors to Controller for its review.
- Insofar as that contract involves the transfer of Controller Personal Data outside of the EEA, incorporate the Standard Contractual Clauses or such other mechanism as directed by the

Controller into the contract between the Processor and each Sub-Processor to ensure the adequate protection of the transferred Controller Personal Data.

- Remain fully liable to the Controller for any failure by each Sub-Processor to fulfil its obligations in relation to the Processing of any Controller Personal Data.
- As of the Addendum Effective Date, the Controller hereby authorises the Processor to engage those Sub-Processors to set out in Annex 3 (Authorised Transfers of Controller Personal Data).

8. Data Subject Rights

Taking into account the nature of the Processing, the Processor shall assist the Controller by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to requests for exercising Data Subject rights as laid down in EU GDPR.

The Processor shall promptly notify the Controller if it receives a request from a Data Subject, the Supervisory Authority and/or other competent authority under any applicable Data Protection Laws with respect to Controller Personal Data.

The Processor shall cooperate as requested by the Controller to enable the Controller to comply with any exercise of rights by a Data Subject under any Data Protection Laws with respect to Controller Personal Data and comply with any assessment, enquiry, notice or investigation under any Data Protection Laws with respect to Controller Personal Data or this Agreement, which shall include:

- The provision of all data requested by the Controller within any reasonable timescale specified by the Controller in each case, including full details and copies of the complaint, communication or request and any Controller Personal Data it holds in relation to a Data Subject.
- Where applicable, providing such assistance as is reasonably requested by the Controller to enable the Controller to comply with the relevant request within the timescales prescribed by the Data Protection Laws.
- Implementing any additional technical and organisational measures as may be reasonably required by the Controller to allow the Controller to respond effectively to relevant complaints, communications or requests.

9. Personal Data Breach

The Processor shall notify the Controller without undue delay and, in any case, within twenty-four (24) hours upon becoming aware of or reasonably suspecting a Personal Data Breach. The Processor will provide the Controller with sufficient information to allow the Controller to meet any obligations to report a Personal Data Breach under the Data Protection Laws. Such notification shall as a minimum:

- Describe the nature of the Personal Data Breach, the categories and numbers of Data Subjects concerned, and the categories and numbers of Personal Data records concerned;
- Communicate the name and contact details of the Processor's Data Protection Officer, Privacy Officer or other relevant contact from whom more information may be obtained;
- Describe the estimated risk and the likely consequences of the Personal Data Breach; and
- Describe the measures taken or proposed to be taken to address the Personal Data Breach.

The Processor shall co-operate with the Controller and take such reasonable commercial steps as are directed by the Controller to assist in the investigation, mitigation and remediation of each Personal Data Breach.

In the event of a Personal Data Breach, the Processor shall not inform any third party without first obtaining the Controller's prior written consent, unless notification is required by EU or Member State law to which the Processor is subject, in which case the Processor shall, to the extent permitted by such law, inform the Controller of that legal requirement, provide a copy of the proposed notification and consider any comments made by the Controller before notifying the Personal Data Breach.

10. Data Protection Impact Assessment and Prior Consultation

The Processor shall provide reasonable assistance to the Controller with any data protection impact assessments which are required under Article 35 of GDPR and with any prior consultations to any supervisory authority of the Controller which are required under Article 36 of GDPR, in each case solely in relation to Processing of Controller Personal Data by the Processor on behalf of the Controller and considering the nature of the processing and information available to the Processor.

11. Erasure or return of Controller Personal Data

The Processor shall promptly and, in any event, within 60 (sixty) calendar days or earlier of: (i) cessation of Processing of Controller Personal Data by Processor; or (ii) termination of the Principal Agreement, at the choice of Controller (such choice to be notified to Processor in writing) either:

- Return a complete copy of all Controller Personal Data to the Controller by secure file transfer in such format as notified by the Controller to the Processor and securely erase all other copies of Controller Personal Data Processed by the Processor or any Authorised Sub-processor; or
- Securely wipe all copies of Controller Personal Data Processed by Processor or any Authorised Sub-processor, and in each case, provide a written certification to the Controller that it has complied fully with the requirements of section Erasure or Return of Controller Personal Data.

Processor may retain Controller Personal Data to the extent required by Union or Member State law, and only to the extent and for such period as required by Union or Member State law, and always provided that Processor shall ensure the confidentiality of all such Controller Personal Data and shall ensure that such Controller Personal Data is only Processed as necessary for the purpose(s) specified in the Union or Member State law requiring its storage and for no other purpose.

12. Audit rights

Processor shall make available to the Controller, upon request, all information necessary to demonstrate compliance with this Addendum and allow for, and contribute to audits, including inspections by the Controller or another auditor mandated by the Controller of any premises where the Processing of Controller Personal Data takes place. The Processor shall permit the Controller or another auditor mandated by the Controller to inspect, audit and copy any relevant records, processes and systems in order that the Controller may satisfy itself that the provisions of this Addendum are being complied with. The Processor shall provide full cooperation to the Controller with respect to any such audit and shall, at the request of the Controller, provide the Controller with evidence of compliance with its obligations under this Addendum. Processor shall immediately inform the Controller if, in its opinion, an instruction infringes the GDPR or other EU or Member State data protection provisions.

13. International Transfers of Controller Personal Data

The Processor shall not process Controller Personal Data nor permit any Authorised Sub-processor to process the Controller Personal Data in a Third Country, other than with respect to those recipients in

Third Countries (if any) listed in Annex 3 (Authorised Transfers of Controller Personal Data), unless authorized in writing by Controller in advance, via an amendment to this Addendum.

When requested by Controller, Processor shall promptly enter into (or procure that any relevant Sub-processor of Processor enters into) an agreement with Controller including Standard Contractual Clauses and/or such variation as Data Protection Laws might require, in respect of any processing of Controller Personal Data in a Third Country, which terms shall take precedence over those in this Addendum.

14. Codes of Conduct and Certification

At the request of the Controller, the Processor shall comply with any Code of Conduct approved pursuant to Article 40 of GDPR and obtain any certification approved by Article 42 of EU GDPR, to the extent that they relate to the processing of Controller Personal Data.

15. General Terms

- Subject to this section, the parties agree that this Agreement and the Standard Contractual Clauses shall terminate automatically upon termination of the Principal Agreement or expiry or termination of all service contracts entered into by the Processor with the Controller, pursuant to the Principal Agreement, whichever is later.
- Any obligation imposed on the Processor under this Addendum in relation to the Processing of Personal Data shall survive any termination or expiration of this Addendum.
- This Addendum, excluding the Standard Contractual Clauses, shall be governed by the governing law of the Principal Agreement for so long as that governing law is the law of a Member State of the European Union.
- Any breach of this Addendum shall constitute a material breach of the Principal Agreement.
- With regard to the subject matter of this Addendum, in the event of inconsistencies between the provisions of this Addendum and any other agreements between the parties, including but not limited to the Principal Agreement, the provisions of this Addendum shall prevail with regard to the parties' data protection obligations for Personal Data of a Data Subject from a Member State of the European Union.
- Should any provision of this Addendum be invalid or unenforceable, then the remainder of this Addendum shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

IN WITNESS WHEREOF, this Addendum is entered into and becomes a binding part of the Principal Agreement with effect from the Addendum Effective Date first set out above.

[Organisation Name] **("Controller")**	[Name] **("Processor")**
Signature: _____	Signature: _____
Name:	Name:
Title:	Title:

Date Signed: Date Signed:

ANNEX 1: DETAILS OF PROCESSING OF CONTROLLER PERSONAL DATA

This Annex 1 includes certain details of the Processing of Controller Personal Data as required by Article 28(3) GDPR.

Subject matter and duration of the Processing of Controller Personal Data

The subject matter and duration of the Processing of the Controller Personal Data are set out in the Principal Agreement and this Addendum.

The nature and purpose of the Processing of Controller Personal Data

[Include description here]

[This could include details of what the Accountant does with the data for example]

The types of Controller Personal Data to be Processed

[Include list of data types here]

[Personal Data for example]

The categories of Data Subject to whom the Controller Personal Data relates

[Include categories of data subjects here – Employees or Parents etc]

ANNEX 2: TECHNICAL AND ORGANISATIONAL MEASURES

1. Organizational security measures

1.1. Security Management

a. Security policy and procedures: Processor must document a security policy with regard to the processing of personal data.

b. Roles and responsibilities：

i. Roles and responsibilities related to the processing of personal data is clearly defined and allocated in accordance with the security policy.

ii. During internal re-organizations or terminations and change of employment, revocation of rights and responsibilities with respective hand-over procedures is clearly defined.

c. Access Control Policy: Specific access control rights are allocated to each role involved in the processing of personal data, following the need-to-know principle.

d. Resource/asset management: Processor has a register of the IT resources used for the processing of personal data (hardware, software, and network). A specific person is assigned the task of maintaining and updating the register (e.g. IT officer).

e. Change management: Processor makes sure that all changes to the IT system are registered and monitored by a specific person (e.g. IT or security officer). Regular monitoring of this process takes place**.**

1.2. Incident response and business continuity

a. Incidents handling / Personal data breaches:

i. An incident response plan with detailed procedures is defined to ensure effective and orderly response to incidents pertaining personal data.

ii. Processor will report without undue delay to Controller any security incident that has resulted in a loss, misuse or unauthorized acquisition of any personal data.

b. Business continuity: Processor establishes the main procedures and controls to be followed in order to ensure the required level of continuity and availability of the IT system processing personal data (in the event of an incident/personal data breach).

1.3. Human resources

a. Confidentiality of personnel: Processor ensures that all employees understand their responsibilities and obligations related to the processing of personal data. Roles and responsibilities are clearly communicated during the pre-employment and/or induction process.

b. Training: Processor ensures that all employees are adequately informed about the security controls of the IT system that relate to their everyday work. Employees involved in the

processing of personal data are also properly informed about relevant data protection requirements and legal obligations through regular awareness campaigns.

2. Technical security measures

2.1. Access control and authentication

a. An access control system applicable to all users accessing the IT system is implemented. The system allows creating, approving, reviewing and deleting user accounts.

b. The use of common user accounts is avoided. In cases where this is necessary, it is ensured that all users of the common account have the same roles and responsibilities.

c. When granting access or assigning user roles, the "need-to-know principle" shall be observed in order to limit the number of users having access to personal data only to those who require it for achieving the Processor's processing purposes.

d. Where authentication mechanisms are based on passwords, Processor requires the password to be at least eight characters long and conform to very strong password control parameters including length, character complexity, and non-repeatability.

e. The authentication credentials (such as user ID and password) shall never be transmitted unprotected over the network.

2.2. Logging and monitoring: Log files are activated for each system/application used for the processing of personal data. They include all types of access to data (view, modification, deletion).

2.3. Security of data at rest

a. Server/Database security

i. Database and applications servers are configured to run using a separate account, with minimum OS privileges to function correctly.

ii. Database and applications servers only process the personal data that are actually needed to process in order to achieve its processing purposes.

b. Workstation security:

i. Users are not able to deactivate or bypass security settings.

ii. Anti-virus applications and detection signatures is configured on a regular basis.

iii. Users don't have privileges to install or deactivate unauthorized software applications.

iv. The system has session time-outs when the user has not been active for a certain time period.

v. Critical security updates released by the operating system developer is installed regularly.

2.4. Network/Communication security:

a. Whenever access is performed through the Internet, communication is encrypted through cryptographic protocols.

b. Traffic to and from the IT system is monitored and controlled through Firewalls and Intrusion Detection Systems.

2.5. Back-ups:

a. Backup and data restore procedures are defined, documented and clearly linked to roles and responsibilities.

b. Backups are given an appropriate level of physical and environmental protection consistent with the standards applied on the originating data.

c. Execution of backups is monitored to ensure completeness.

2.6. Mobile/Portable devices:

a. Mobile and portable device management procedures are defined and documented establishing clear rules for their proper use.

b. Mobile devices that are allowed to access the information system is pre-registered and pre-authorized.

2.7. Application lifecycle security: During the development lifecycle, best practice, state of the art and well acknowledged secure development practices or standards is followed.

2.8. Data deletion/disposal:

a. Software-based overwriting will be performed on media prior to their disposal. In cases where this is not possible (CD's, DVD's, etc.) physical destruction will be performed.

b. Shredding of paper and portable media used to store personal data is carried out.

2.9. Physical security: The physical perimeter of the IT system infrastructure is not accessible by non-authorized personnel. Appropriate technical measures (e.g. Intrusion detection system, chip-card operated turnstile, single-person security entry system, locking system) or organizational measures (e.g., security guard) shall be set in place to protect security areas and their access points against entry by unauthorized persons.

ANNEX 3: AUTHORISED TRANSFERS OF CONTROLLER PERSONAL DATA

List of Approved Sub-processors as at the Addendum Effective Date to be included here. Please include (i) full legal name; (ii) processing activity; (iii) location of service centre(s).

No.	Authorizes sub- processor (full legal name)	Processing activity	Location of service centre(s).
1.			