



Feidhmeannacht na Seirbhíse Sláinte
Health Service Executive

***Out of State (UK) Service Provider
Data Processing Terms***

Between

Health Service Executive (as Controller)

And

Provider (as Processor)

DATA PROCESSING TERMS (PROVIDER TO HSE)

RECITALS

- A.** These data processing terms constitute the Parties' data processing agreement for the purposes of Article 28 of the GDPR or the UK GDPR as the case may be.
- B.** These data processing terms apply in conjunction with the service level agreement entered into between the parties for the provision of services by the Provider to the Executive outside the State (the "**Arrangement**").
- C.** The Parties acknowledge and agree that, for the purposes of Data Protection Legislation, and the Processing of the Personal Data as anticipated by these Terms, the Executive is the Controller and the Provider is the Processor.
- D.** Appendix 1 of these Terms contains a description of the subject matter, duration of the Processing, nature and Purpose of the Processing, as well as the type of Personal Data and categories of Data Subjects Processed by the Service Provider under these Terms.
- E.** These Terms cover the Provider's Processing of any and all HSE Personal Data under the Arrangement to the extent that such Processing is not already covered by an existing data processing agreement in place for this purpose (i.e. in the form of the HSE Data Processing Agreement and or Data Sharing Agreement available on the Executive's website).
- F.** To the extent that the parties are independent controllers then their Processing of Personal Data will be governed by the terms of Clause 26 of the Arrangement and these Terms shall not apply.
- G.** To the extent that there is any conflict between these Terms and the provisions of the Arrangement, then the Arrangement shall prevail.

TERMS

1 DEFINITIONS:

Terms not otherwise defined in these Terms will have the meaning as set forth in the Arrangement. The following definitions apply in these Terms (including the Recitals above), unless the context otherwise requires:

Arrangement as defined in Recital B;

Data Controller or **Controller** has the meaning given to that term in Article 4 of the GDPR or the UK GDPR as the case may be;

Data Processor or **Processor** has the meaning given to that term in Article 4 of the GDPR or the UK GDPR as the case may be;

Data Protection Commission means the Supervisory Authority in Ireland for the purposes of Article 51 of the GDPR whose principal administrative offices are at 21 Fitzwilliam Square South, Dublin 2, D02

RD28, Ireland, or any replacement Supervisory Authority under Data Protection Legislation, appointed from time to time in Ireland;

Data Protection Impact Assessment has the meaning given to that term in Clause 3.1 of these Terms;

Data Protection Legislation means all applicable legislation relating to Personal Data and privacy, including the Data Protection Acts, 1988-2018, the Data Sharing and Governance Act 2019, the General Data Protection Regulation (EU) 2016/679 (the “**GDPR**”), the Privacy and Electronic Communications Directive 2002/58/EC (as updated by Directive 2009/136/EC) and the European Communities (Electronic Communications, Networks and Services) (Privacy and Electronic Communications) Regulations 2011 (S.I. 336/2011) the UK Data Protection Act 2018 and the UK GDPR (as retained by section 3(10) (as supplemented by section 205(4)) of the UK DPA) (“**UK GDPR**”), and any secondary legislation, including any statutory instrument, order, rule or regulation, made thereunder and any regulations or other legislative measures and/or implemented and/or delegated acts thereunder;

Data Subject has the meaning given to that term in Article 4(1) of the GDPR or the UK GDPR as the case may be;

Delete, Deleted, Deletion and like words, shall mean the permanent removal of data and all traces of the data, by means of the physical destruction of the data, or the physical destruction of the medium used to store the data, or the overwriting of the data, in accordance with internationally accepted data erasure standards using data sanitation software;

EEA shall mean the states that are contracting parties to the Agreement on the European Economic Area from time to time;

HSE Personal Data shall mean the Personal Data and Special Categories of Personal Data Processed for the Purpose by the Provider on behalf of the Executive as more specifically detailed in Appendix 1 of these Terms;

Information Commissioner’s Office means the Supervisory Authority in the UK for the purposes of Article 51 of the UK GDPR whose principal administrative offices are at Water Lane, Wycliffe House Wilmslow - Cheshire SK9 5AF United Kingdom or any replacement Supervisory Authority under Data Protection Legislation, appointed from time to time in the U.K.;

Personal Data has the meaning given to that term in Article 4 of the GDPR or the UK GDPR as the case may be;

Personal Data Breach has the meaning given to that term in Article 4 of the GDPR or the UK GDPR as the case may be;

Processing, Process and like words, have the meaning given to those terms in Article 4 of the GDPR or the UK GDPR as the case may be;

Purpose shall mean the purpose of the Processing as more specifically detailed in Appendix 1 of these Terms and for the avoidance of doubt is not any other purpose or purposes for which the Provider may Process Personal Data and Special Categories of Personal Data as Data Controller such as, for example, the provision of treatment and care to Data Subjects;

Services has the meaning given to that term in the Arrangement;

Special Categories of Personal Data has the meaning given to that term in Article 9(1) of the GDPR or the UK GDPR as the case may be;

Standard Contractual Clauses The contractual clauses dealing with the transfer of Personal Data outside the EEA, which have been approved by (i) the European Commission under Data Protection Legislation, or (ii) by the Data Protection Commission or an equivalent Supervisory Authority under Data Protection Legislation as may be revised, updated or replaced from time to time; and in relation to a transfer of Personal Data from the UK, the EU SCCs in conjunction with and as varied by the United Kingdom Addendum B.1.0 to the Standard Contractual Clauses issued by the UK Information Commissioner's Office as may be revised, updated or replaced from time to time;

Sub-Processors shall mean any person or legal entity which is not party to the Arrangement or other contract(s) between the Executive and the Provider, and which is engaged by the Provider to perform any or all of its obligations in relation to the Processing of HSE Personal Data, including for the avoidance of doubt, a Provider group company including subsidiaries and affiliates;

Supervisory Authority has the meaning given to that term in Article 4 of the GDPR or the UK GDPR as the case may be and in Ireland, is the Data Protection Commission and in the UK is the Information Commissioner's Office;

Terms shall mean these Data Processing Terms;

Transfer Impact Assessment has the meaning given to that term in Clause 6.3 of these Terms; and

UK The United Kingdom of Great Britain and Northern Ireland.

2 Obligations of the Provider

2.1 To the extent that the Provider Processes HSE Personal Data for the Purpose as a Data Processor on behalf of the Executive, the Provider shall:

2.1.1 comply at all times with their obligations as a Data Processor as set out in Data Protection Legislation and these Terms, and not undertake any actions or permit any actions to be undertaken on their behalf which may cause the Executive to be in breach of Data Protection Legislation;

2.1.2 manage and Process any HSE Personal Data they acquire from the Executive solely in accordance with the documented instructions of the Executive as set out in these Terms, including with regard to transfers of HSE Personal Data to a third country or an international organisation, unless required to do so by European Union or Irish law to which the Provider is subject; in such a case, the Provider shall inform the Executive in writing of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest;

2.1.3 notify the Executive prior to carrying out any instruction from the Executive if, in the Provider's opinion, such instruction is likely to result in Processing that is in breach of the Arrangement (including these Terms) or Data Protection Legislation;

2.1.4 only Process and use HSE Personal Data for the purpose of providing the Services to, on behalf of or for the Executive and, not otherwise modify, amend or alter the contents of HSE Personal Data unless specifically authorised to do so in writing by the Executive;

- 2.1.5 take all reasonable measures to ensure the reliability of any of the Provider's employees and contractors who have access to HSE Personal Data;
- 2.1.6 ensure that access to HSE Personal Data is limited to those of the Provider's employees and contractors who need to have access to it, and that they are informed of the confidential nature of the HSE Personal Data, are under an obligation to keep such HSE Personal Data confidential, and comply with the obligations set out in these Terms;
- 2.1.7 ensure that all the relevant Provider employees and contractors with access to HSE Personal Data have been provided with and have undergone appropriate Data Protection and IT security training;
- 2.1.8 ensure they have appropriate procedures in place which prevent the Provider's employees and contractors from downloading HSE Personal Data from the Provider's IT devices and servers and storing this HSE Personal Data on the employees' or contractors' personal IT devices (i.e. where the IT device is the personal property of the employee or contractor and not the Provider);
- 2.1.9 ensure they have appropriate processes implemented and documented which will allow the Provider to promptly and effectively detect, contain, analyse, respond and recover from any suspected or actual information security and cyber security incidents within their organisation, and where necessary to promptly notify the Executive of any such incidents involving HSE Personal Data;
- 2.1.10 ensure all printouts taken by the Provider's employees and contractors containing HSE Personal Data are managed and stored appropriately and, disposed of securely when they are no longer required;
- 2.1.11 not disclose or permit the disclosure of any the HSE Personal Data to any third party unless specifically authorised to do so in writing by the Executive. In the event that the Provider is legally required to disclose any HSE Personal Data to a third party, the Provider undertakes to notify the Executive of such requirement prior to any disclosure and, unless prohibited by law, to supply the Executive with copies of all communications between the Provider and any third party to which such disclosure is made. At the request of the Executive, the Provider shall co-operate with the Executive in bringing any legal or other proceedings to challenge the validity of the requirement to disclose the HSE Personal Data;
- 2.1.12 taking into account the nature of Processing and subject to applicable law, assist the Executive by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Executive's obligations to respond to requests from Data Subjects exercising their rights under Data Protection Legislation, in particular, Chapter III of the GDPR or the UK GDPR as the case may be (including their right of access, rectification of and erasure of their Personal Data). Upon a request from the Executive for such assistance, the Provider shall comply with the request in a timely manner, so as to allow the Executive to comply with its legal obligations concerning the timescales for responding to such requests from Data Subjects, as laid down in Article 12 of the GDPR or the UK GDPR as the case may be; and
- 2.1.13 without prejudice to Clause 21 (Complaints) or Clause 29.4 (Data Protection) of the Arrangement, assist the Executive in relation to any assessment, enquiry, notice or investigation received by the Executive from a Supervisory Authority which may include (as

appropriate) the provision of data requested by the Executive within the timescales reasonably specified by the Executive in each case.

3 Data Protection Impact Assessments

3.1 Without prejudice to Clause 10 (Information Requirements) of the Arrangement, taking into account the nature of Processing and the information available to the Provider, the Provider shall provide all reasonable assistance to the Executive in the preparation of any assessment by the Executive of the impact of the envisaged Processing on the protection of HSE Personal Data ("**Data Protection Impact Assessment**"), prior to commencing any Processing. Such assistance may, at the discretion of the HSE, include the following:

- 3.1.1 a systematic description of the envisaged Processing operations and the purpose of the Processing;
- 3.1.2 an assessment of the necessity and proportionality of the Processing operations in relation to the Services;
- 3.1.3 an assessment of the risks to the rights and freedoms of Data Subjects; and
- 3.1.4 the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of HSE Personal Data.

4 Technical & Operational Measures

4.1 The Provider shall implement appropriate technical and organisational measures to protect against the accidental or unlawful destruction, loss alteration, unauthorised disclosure of, or access to HSE Personal Data processed by the Provider.

4.2 Where the Provider uses their own ICT resources (i.e. ICT resources which are owned or controlled by the Provider) to Process or store HSE Personal Data, the Provider must implement the minimum technical and organizational measures set out in Appendix 2 of these Terms to protect the HSE Personal Data and ensure such measures are included in any procurement subject to Clause 10 (ICT) of the Arrangement.

4.3 At the written request of the Executive, the Provider shall provide the Executive within seven (7) calendar days, with a written description of the technical and organisational measures implemented by the Provider and (as applicable) their Sub-Processors to protect HSE Personal Data they Process.

5 Appointment of Sub-Processors

5.1 The Provider shall not engage any Sub-Processors to Process HSE Personal Data other than with the prior written consent of the Executive.

5.2 The Provider shall inform the Executive in writing of any intended changes concerning the addition or replacement of other Sub-Processors who will Process HSE Personal Data, thereby giving the Executive the opportunity to object to such changes where it considers that such Sub-Processors do not provide sufficient guarantees under Data Protection Legislation. In the event that the Executive objects to the addition or replacement of Sub-Processors, the Provider shall use reasonable endeavours to address the Executive's concerns.

5.3 Where the Provider engages a Sub-Processor to Process HSE Personal Data, the Provider shall impose obligations on the Sub-Processor, by way of a written contract / agreement between the Provider and the Sub-Processor, which includes terms that are the same as, or equivalent to those terms set out in these Terms. The Provider shall ensure that Sub-Processors engaged by them to Process HSE Personal Data, cease Processing HSE Personal Data upon the earlier termination of these Terms or the termination of the Provider's contract / agreement with the Sub- Processor. The Provider shall remain fully liable to the Executive for any failure by a Sub-Processor to fulfil its obligations in relation to the Processing of any HSE Personal Data.

6 International Data Transfers

6.1 The Provider shall not process and/or transfer any HSE Personal Data in or to any country outside the EEA or the UK without the prior written consent of the Executive.

6.2 Where the Executive has consented to the Provider Processing and/or transferring HSE Personal Data in or to a country outside the EEA or the UK as the case may be, the Provider may only Process and/or transfer HSE Personal Data in or to:

6.2.1 a country outside the EEA or UK in respect of which an adequacy decision made by the European Commission under Article 45(3) of the GDPR or the UK GDPR as the case may be is in force; or

6.2.2 a country outside the EEA or UK subject to the execution of Standard Contractual Clauses or other appropriate safeguards under Article 46 of the GDPR or the UK GDPR as the case may be as between the Provider and a Sub-Processor approved in accordance with Clause 5 of these Terms, where the Provider is transferring the HSE Personal Data (i.e. it is the data exporter) and the Sub-Processor is receiving the HSE Personal Data (i.e. it is the data importer); or

6.2.3 a country outside the EEA or UK but where the transferee (i.e. the data importer) of the HSE Personal Data is a parent or subsidiary company of the Provider, approved in accordance with Clause 5, provided that the Provider and that parent or subsidiary company have adopted Binding Corporate Rules which have been approved by the relevant national Supervisory Authority under Article 47 of the GDPR or the UK GDPR as the case may be.

6.3 For the purposes of Clause 6.2.2 above, the Provider shall undertake and document a risk assessment on the laws and practices in force within the country outside the EEA or the UK where the data importer is located (a "**Transfer Impact Assessment**"), and where necessary implement supplementary measures and shall, upon request, make available to the Executive a copy of the Transfer Impact Assessment, and provide details of any supplementary measures implemented.

6.4 Upon the written request of the Executive, the Provider shall supply the Executive within fourteen (14) calendar days, with a complete list of all countries around the world, where the Provider and (as applicable) its Sub-Processors are currently processing HSE Personal Data.

6.5 In the event that the transfer mechanism entered into under this Clause 6 of these Terms ceases to be valid, the Provider shall at the Executive's discretion:

6.5.1 enter into and/or procure that any relevant Sub-Processor enters into an appropriate alternative data transfer mechanism;

- 6.5.2 delete any HSE Personal Data in its and/or its Sub-Processor's possession; or
- 6.5.3 return any HSE Personal Data in its and/or its Sub-Processor's possession to the Executive.

7 Breach Notifications

- 7.1 The Provider shall notify the Executive in writing, without undue delay, and at the latest within twenty-four (24) hours, after the Provider or (as applicable) their Sub-Processors become aware of a Personal Data Breach within their respective organisations which affects any HSE Personal Data which is Processed by the Provider or (as applicable) their Sub-Processors.
- 7.2 When notifying the Executive of a Personal Data Breach, the Provider shall ensure the notification includes, at a minimum, the information listed in Article 33(3) of the GDPR or the UK GDPR as the case may be.

8 Audit

- 8.1 The Provider shall keep accurate and up-to-date records relating to its Processing of HSE Personal Data.
- 8.2 The Provider shall make available to the Executive all information necessary to demonstrate the Provider's compliance with the obligations laid down in Article 28 of the GDPR or the UK GDPR as the case may be and allow for and contribute to audits and/or inspections carried out in accordance with Clause 12 (Access Rights) of the Arrangement.

9 Termination or Completion of the Arrangement

- 9.1 Without affecting indemnity, other right or remedy available to the Executive, a breach by the Provider of any of the terms of these Terms shall be deemed a "serious breach" within the meaning of Clauses 34.1 and 34.6 (Termination or Expiry) of the Arrangement and where that breach is irremediable or if such breach is remediable and the Provider fails to remedy that breach within thirty (30) calendar days after being notified by the Executive to do so.
- 9.2 Upon termination or the completion of the Arrangement for any reason (including but not limited to in circumstances of insolvency, receivership or any analogous circumstances affecting the Provider), the Provider shall, at the request and choice of the Executive and at the cost of the Provider, Delete or return to the Executive, all HSE Personal Data held by the Provider and (as applicable) their Sub-Processors solely for the Purpose:
 - 9.2.1 where the Executive has requested the Provider Delete the HSE Personal Data, the Provider shall ensure all HSE Personal Data and all the copies thereof (irrespective of format) held by the Provider and (as applicable) their Sub-Processors is Deleted from all of the Provider's and (as applicable) their Sub-Processors' IT systems, IT devices, mobile computer devices, removable storage devices and servers within thirty (30) calendar days. The Provider shall notify the Executive in writing, when they and (as applicable) their Sub-Processors have completed the Deletion process;
 - 9.2.2 where the Executive has requested the Provider return the HSE Personal Data, the Provider shall ensure all HSE Personal Data and all the copies thereof (irrespective of format) held by the Provider and (as applicable) their Sub-Processors is returned to the Executive within thirty (30) calendar days. The Provider shall ensure all HSE Personal Data held electronically

by the Provider and (as applicable) their Sub-Processors is returned to the Executive in a commonly used electronic format; and

9.2.3 in circumstances where, after the termination or completion of the Arrangement, the Provider is required under European Union or Irish law to retain a copy of any HSE Personal Data, the Provider undertakes to supply the Executive in writing, unless prohibited by law, with the full details of any HSE Personal Data they are legally required to retain and the details of the European Union or Irish law governing this requirement. In such circumstances, the Provider shall ensure all HSE Personal Data is appropriately secured and encrypted at all times to a standard which is satisfactory to the Executive and shall ensure that the HSE Personal Data is only processed for the specific legal retention purpose so-notified to the Executive. When the Provider is no longer legally required to retain the HSE Personal Data, the Provider shall, at the request and choice of the Executive, Delete or return to the Executive, the HSE Personal Data in accordance with Clauses 9.2.1 and 9.2.2 of these Terms.

9.3 Upon termination or the completion of the Arrangement, the Provider shall return to the Executive with immediate effect, all Executive IT devices, mobile computer devices, removable storage devices, phones, parking permits, I.D. badges and any other equipment which the Executive provided to the Provider's employees and contractors.

10 Indemnity

10.1 Notwithstanding any other provision of these Terms, the Provider hereby indemnifies and holds harmless, and agrees to keep indemnified and hold the Executive harmless against all damages, losses, liabilities, costs, fines and/or penalties, expenses, compensation and associated costs arising out of or in connection with any act, omission, default or negligence of the Provider and its Sub-Processors relating to the Processing of HSE Personal Data under these Terms.

11 Survival of Obligations

11.1 All the obligations under these Terms shall survive and continue after termination, and will bind the Provider's legal representatives, successors and assigns, until such time as all the HSE Personal Data has been returned to the Executive or permanently destroyed.

12 Consequences of Breach

12.1 Without affecting indemnity, other right or remedy available to the Executive, a breach by the Provider of any of the provisions of these Terms shall be deemed a "serious breach" within the meaning of Clauses 34.1 and 34.6 (Termination or Expiry) of the Arrangement, where that breach is irremediable or if such breach is remediable and the Provider fails to remedy that breach within thirty (30) calendar days after being notified by the Executive to do so.

13 Variation

13.1 The Executive may implement reasonable variations to these Terms from time to time, including but not limited to amendments required to reflect any changes in laws, including Data Protection Legislation or practice and/or Executive policy and which will be made available to the Provider on the HSE website.

APPENDIX 1

The data processing activities carried out by the Provider pursuant to the Terms are described as follows:

1 Subject Matter of the Processing

The Provider is under contract to provide one or more Services to, on behalf of and/or for the Executive. The provision of these Services necessitates the Provider Processing data including Personal Data on behalf of the Executive.

2 Duration of the Processing

The HSE Personal Data shall be Processed by the Provider for as long as necessary and in accordance with the HSE Data Retention Policy (which may be amended from time to time). The duration of the Processing shall correspond to the terms of the Arrangement for the Services between the Provider and the Executive.

3 Nature of the Processing

Depending on the Service(s) provided by the Provider to the Executive, the Personal Data may be subject to the following basic Processing activities:

- Receive data, including collection, accessing, retrieval, recording and data entry.
- Hold data, including storage, hosting, organisation and structuring.
- Use data, including analysing, consultation, migrating and testing.
- Update data, including correcting, adaptation, alteration, alignment and combination.
- Send data, including electronic transmission and sending by other means.
- Protect data, including restricting, encrypting, and security testing.
- Share data, including disclosure, dissemination, allowing access or otherwise making data available.
- Backup data, including taking, storing and restoration of data.
- Erase data, including destruction and deletion.

4 Purpose of the Processing

The Provider shall only Process HSE Personal Data as necessary to provide the Services pursuant to the Arrangement between the Executive and the Provider, these Terms and as further instructed by the Executive.

5 Description of the HSE Personal Data (if applicable) Processed

Depending on the Service(s) provided by the Provider to the Executive, the Provider whilst providing the Service(s) to, on behalf of and/or for the Executive, may Process the following categories of Personal Data and Special Categories of Personal Data:

Personal Data, which may include, but is not limited to the following:

- First and Last name
- Title
- Position
- Date of Birth
- Home contact details (address, telephone number, mobile number, personal email address)
- Business contact details (address, telephone number, mobile number, personal email address, work location)
- Family life
- Civil Partnership and Marital status
- Employer name & address
- Employee number
- Personal Public Service Number (PPSN)
- Individual Health Identifier (DTI)
- Medical Record Number (MRN)
- Personal life data
- Professional life data
- Connection data
- Location data
- Financial and bank details
- Employment details
- Education details
- General Practitioner contact details (name, address, contact telephone number)

Special Categories of Personal Data, which may include, but is not limited to the following:

- Religious or philosophical beliefs
- Trade union membership
- Data concerning health
- Sex life or sexual orientation
- Biometric data
- Genetic data

6 Categories of Data Subjects whose Personal Data is processed

Depending on the Service(s) provided by the Provider to the Executive, the Provider whilst providing the Services to the Executive, may Process Personal Data relating to the following categories of Data Subjects:

- Current, former and prospective staff and contractors of the Executive
- Agency staff and contractors of the Executive
- Patients, clients and service users, or their parents, next of kin, legal guardians or attorneys, of the Executive
- Agency patients, clients and service users or their parents, next of kin, legal guardians or attorneys
- Business partners, service providers and suppliers (who are natural persons) of the Executive
- Staff and contractors (who are natural persons) of business partners, service providers and suppliers of the Executive

APPENDIX 2

The minimum technical and organisational measures that must be implemented by the Provider when using their own ICT resources to Process HSE Personal Data:

- 1 All IT Networks (with the exception of those which are owned or controlled by the Executive) used by the Provider to Process or store any HSE Personal Data have properly managed, configured and up to date firewalls in place;
- 2 All IT Networks (with the exception of those which are owned or controlled by the Executive) used by the Provider to Process or store HSE Personal Data have properly managed and configured network monitoring and logging in place;
- 3 All IT Networks (with the exception of those which are owned or controlled by the Executive) used by the Provider to Process or store HSE Personal Data have properly managed, configured and up to date intrusion detection and/or intrusion prevention systems in place;
- 4 All IT Networks (with the exception of those which are owned or controlled by the Executive) used by the Provider to Process or store HSE Personal Data have strong access controls in place;
- 5 Appropriate levels of network, system, and physical redundancy are in place;
- 6 All the buildings or facilities (with the exception of those which are owned or controlled by the Executive) used by the Provider to host IT systems, IT devices, servers and other critical IT equipment which are used to Process or store HSE Personal Data are protected by appropriate physical and environmental controls;
- 7 All IT devices, mobile computer devices and servers (with the exception of those which are owned or controlled by the Executive) used by the Provider to Process or store HSE Personal Data have real-time protection anti-virus, anti-malware and anti-spyware software installed and updated daily;
- 8 All IT systems, IT devices, mobile computer devices, servers and other critical IT equipment (with the exception of those which are owned or controlled by the Executive) used by the Provider to Process or store HSE Personal Data are protected by strong unique passwords which satisfy or better the requirements of the HSE Password Standards Policy (<https://www.hse.ie/eng/services/publications/pp/ict/>);
- 9 All the mobile computer devices and removable storage devices (with the exception of those which are owned or controlled by the Executive) used by the Provider to Process or store HSE Personal Data have encryption enabled which encrypts any HSE Personal Data stored at rest on the device. The encryption of the HSE Personal Data on the device may be achieved by either full-disk encryption, file system encryption or (as applicable) database encryption. All encryption used by the Provider must satisfy or better the requirements of the HSE Encryption Policy (<https://www.hse.ie/eng/services/publications/pp/ict/>);
- 10 All servers (with the exception of those which are owned or controlled by the Executive) used by the Provider to Process or store HSE Personal Data have encryption enabled which encrypts any HSE Personal Data stored at rest on the server. The encryption of the HSE Personal Data on the server may be achieved by either full-disk encryption, file system encryption or (as applicable) database encryption. All encryption used by the Provider must satisfy or better the requirements of the HSE Encryption Policy (<https://www.hse.ie/eng/services/publications/pp/ict/>);
- 11 All servers (with the exception of those which are owned or controlled by the Executive) used by the Provider to Process or store HSE Personal Data are backed up on a daily basis. Where the Provider backs up the servers onto backup media, the Provider must ensure the following:

- 11.1 The backup media is stored a sufficient distance away from the server, for example, in another building on-site under the control of the Provider or off-site in a building or facility controlled by the Provider or a contracted third party;
- 11.2 When not in use, the backup media is protected from damage caused by fire, heat, humidity, water and exposure to strong magnetic fields;
- 11.3 The backup media is password protected by strong unique passwords which satisfy or better the requirements of the HSE Password Standards Policy (<https://www.hse.ie/eng/services/publications/pp/ict/>);
- 11.4 The backup media is encrypted using strong encryption which satisfies or better the requirements of the HSE Encryption Policy (<https://www.hse.ie/eng/services/publications/pp/ict/>);
- 11.5 Access to the backup media is limited to the Providers employees, contractors and/or (as applicable) Sub-Processors who are involved in the backup process;
- 11.6 When in transit, the backup media is protected at all times from damage, theft, interference and loss;
- 11.7 The backup media is tested by the Provider on a regular basis;
- 11.8 All old, obsolete and damaged backup media which was used to backup HSE Personal Data is physically destroyed.
- 12 All servers (with the exception of those which are owned or controlled by the Executive) used by the Provider to Process or store HSE Personal Data have logging enabled, and the server logs are monitored by the Provider on a regular basis;
- 13 All HSE Personal Data which is sent in transit by the Provider is sent via secure channels (for example, VPN, Secure FTP or TLS) or encrypted email. All encryption used by the Provider must satisfy or better the requirements of the HSE Encryption Policy (<https://www.hse.ie/eng/services/publications/pp/ict/>);
- 14 Appropriate patch management procedures are in place for managing the timely application of relevant security software updates and patches to all IT devices, mobile computer devices, servers and other critical IT equipment (with the exception of those which are owned or controlled by the Executive) used by the Provider to Process or store HSE Personal Data;
- 15 Documented disaster recovery plans are in place which detail how the Provider will restore the availability of, and access to any servers (with the exception of those which are owned or controlled by the Executive) used by the Provider to Process or store HSE Personal Data in the event of a physical or technical security breach;
- 16 Appropriate asset management procedures are in place which allow for the management and recording of all the Providers IT hardware and software assets used to Process or store HSE Personal Data;
- 17 Appropriate procedures are in place for the timely decommissioning and secure wiping or destruction (i.e. process that renders data unrecoverable) of all old, obsolete and damaged IT devices, mobile computer devices, servers, software and other critical IT equipment (with the exception of those which are owned or controlled by the Executive) used by the Provider to Process or store HSE Personal Data;
- 18 Appropriate procedures are in place which allow the Provider to regularly, test, assess and evaluate the effectiveness of the technical and organisational measures they have implemented to ensure the security of HSE Personal Data which they Process on behalf of the Executive;

- 19 Appropriate separation controls are in place which provide for the separation of different customers data on the Providers IT hardware and software and ensure HSE Personal Data is Processed by the Provider as separately as possible from the Providers other customer's data;
- 20 Full separation (where applicable) of the Providers production and development / test / training environments is in place;
- 21 Documented IT and information security policies are in place which all the Provider's employees and contractors sign up to, and are expected to comply with;
- 22 Appropriate procedures are in place for the vetting of all new Provider employees and contractors who will have access to HSE Personal Data;
- 23 Non-disclosure and confidentiality clauses are included in the Providers contracts of employment for all their employees and contractors who have access to HSE Personal Data;
- 24 Where legally required to do so, the Provider has appointed a Data Protection Officer (DPO) in accordance with Article 37 of the GDPR or the UK GDPR as the case may be.