THIS DATA PROTECTION ADDENDUM FORMS PART OF THE AGREEMENT FOR THE PROVISION OF DOSIMETRY SERVICES THAT GOVERN THE SUPPLY OF THE DOSIMETRY SERVICES

1. DEFINITIONS AND INTERPRETATION

1.1 Definitions

In this Addendum, the following terms shall have the following meanings:

"**Agent**" means LANDAUER EUROPE, Ltd, a company registered in the UK, having its main place of business at Unit 28, Bankside, Station Approach, Kidlington, Oxford, OX5 1JE, UK, and the agent of the Provider that promotes and sells the Dosimetry Services in certain territories, in particular UK and the Republic of Ireland, and interacts and communicates with Clients and potential clients on behalf of the Provider.

"**Client**" means the purchaser of the Dosimetry Services;

"**Provider**" means LANDAUER, Inc, a company incorporated in the state of Delaware, USA, having its main place of business at 2, Science Road, Glenwood, IL 60425, USA, and the provider of the Dosimetry Services under these Terms.

"**Dosimetry Services**" means the dosimetry services provided by Provider;

"**Terms**" means the terms and conditions of the agreement that governs the supply of the Dosimetry Service by the Supplier to the Client.

"**Appropriate Safeguards**" means such legally enforceable mechanism(s) for transfers of Personal Data as may be permitted under Data Protection Laws from time to time;

"**Data Processing Losses**" means all liabilities, including all:

(a) costs (including legal costs), claims, demands, actions, settlements, charges, procedures, expenses, losses and damages (including relating to material or non-material damage); and

(b) to the extent permitted by Applicable Law:

(i) administrative fines, penalties, sanctions, liabilities or other remedies imposed by a Supervisory Authority;

(ii) compensation to a Data Subject ordered by a Supervisory Authority; and

(iii) the reasonable costs of compliance with investigations by a Supervisory Authority;

"**Data Protection Laws**" means as applicable and binding on the Client, the Provider or the Dosimetry Services:

(a) in the UK:

(i) the Data Protection Act 1998 ("**DPA 1998**") and any laws or regulations implementing Council Directive 95/46/EC ("**Data Protection Directive**"); and/or

(ii) the Regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) ("**GDPR**"), and/or any corresponding or equivalent national laws or regulations ("**Revised UK DP Law**");

(b) in other EU countries: the Data Protection Directive or the GDPR, once applicable, and all relevant Member State laws or regulations giving effect to or corresponding with them;

"**Data Subject Request**" means a request made by a Data Subject to exercise any rights of Data Subjects under Data Protection Laws;

"**Complaint**" means a complaint or request relating to either party's obligations under Data Protection Laws relevant to these Terms, including any compensation claim from a Data Subject or any notice, investigation or other action from a Supervisory Authority;

"**DPIA**" means a data protection impact assessment, in accordance with Data Protection Laws;

"**GDPR Date**" means from when the GDPR applies on 25 May 2018;

"**Personal Data Breach**" means any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, any Protected Data;

"**Price List**" means the Provider's price list for the Dosimetry Services in force as updated from time to time;

"**Protected Data**" means Personal Data received from or on behalf of the Client in connection with the performance of the Provider's obligations under these Terms;

"**Sub-Processor**" means another Data Processor engaged by the Provider for carrying out processing activities in respect of the Protected Data on behalf of the Client;

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

1.2 Interpretation

In this Addendum:

1.2.1 "**Data Controller**" (or "controller"), "**Data Processor**" (or "processor"), "**Data Subject**", "**international organisation**", "**Personal Data**" and "**processing**" all have the meanings given to those terms in Data Protection Laws (and related terms such as "**process**" have corresponding meanings);

1.2.2 references to the DPA 1998 or the Data Protection Directive and to terms defined in that Act or in that Directive shall be replaced with or incorporate (as the case may be) references to any laws replacing, amending, extending, re-enacting or consolidating such Act or Directive (including the GDPR) and the equivalent terms defined in such laws, once in force and applicable;

1.2.3 to the extent that a term of this Addendum requires the performance by a party of an obligation "in accordance with Data Protection Laws" (or similar), unless otherwise expressly agreed in this Addendum, this requires performance in accordance with the relevant requirements of such Data Protection Laws as are in force and applicable at the time of performance (if any);

2. DATA PROTECTION

2.1 Processor/Controller

2.1.1 The parties agree that, for the Protected Data, the Client shall be the Data Controller and the Provider shall be the Data Processor.

2.2 Compliance with Data Protection Laws and obligations

2.2.1 the Provider shall process Protected Data in compliance with:

(a) the obligations of Data Processors under Data Protection Laws, in respect of the performance of its obligations under these Terms; and

(b) these Terms.

2.2.2 The Client shall comply with:

(a) all Data Protection Laws in connection with the processing of Protected Data, the Dosimetry Services and the exercise and performance of its respective rights and obligations under these Terms, including maintaining all relevant regulatory registrations and notifications as required under Data Protection Laws; and

(b) these Terms.

2.2.3 The Client warrants, represents and undertakes, that:

(a) with respect to data being provided to or accessed by the Provider for the performance of the Dosimetry Services under these Terms, such data shall have been sourced by the Client in all respects in compliance with Data Protection Laws, including in terms of its collection, storage and processing, which for the avoidance of doubt includes the Client providing all required fair processing information to, and obtaining all necessary consents from, Data Subjects;

(b) all instructions given by it to the Provider in respect of Personal Data shall at all times be in accordance with Data Protection Laws;

(c) it has undertaken due diligence in relation to the Provider's processing operations, and it is satisfied that:

(i) the Provider's processing operations are suitable for the purposes for which the Client proposes to use the Dosimetry Services and engage the Provider to process the Protected Data; and

(ii) the Provider has sufficient expertise, reliability and resources to implement technical and organisational measures that meet the requirements of Data Protection Laws.

2.2.4 The Client shall not unreasonably withhold, delay or condition its agreement to any Change requested by the Provider in order to ensure the Dosimetry Services and the Provider (or any Sub-Processor) can comply with Data Protection Laws, and no longer than 1 month.

2.3 Details of processing and instructions

2.3.1 Insofar as the Provider processes Protected Data on behalf of the Client, the Provider:

(a) unless required to do otherwise by Applicable Law, shall, and shall take steps to ensure each person acting under its authority shall, process the Protected Data only on and in accordance with the Client's documented instructions as set out in this clause 2 and schedule 2 (*Data Processing Details*), as updated from time to time;

(b) if Applicable Law requires it to process Protected Data other than in accordance with the Processing Instructions, shall notify the Client of any such requirement before processing the Protected Data unless Applicable Law prohibits such information on important grounds of public interest; and

(c) shall inform the Client if the Provider becomes aware of a Processing Instruction that, in the Provider's opinion, infringes Data Protection Laws:

(i) provided that doing so shall be without prejudice to clauses 2.2.2 and 2.2.3;

(ii) it being agreed that to the maximum extent permitted by mandatory law, the Provider shall have no liability howsoever arising (whether in contract, tort (including negligence) or otherwise) for any losses, costs, expenses or liabilities (including any Data Processing Losses) arising from or in connection with any processing in accordance with the Client's Processing Instructions following the Provider informing the Client of an infringing Processing Instruction; and

(iii) it being understood that this clause 1.1.1(c) shall only apply from the GDPR Date.

2.3.2 The processing of Protected Data to be carried out by the Provider under these Terms shall comprise the processing set out in schedule 2 (*Data Processing Details*), as may be updated from time to time.

2.4 Technical and organisational measures

2.4.1 The Provider shall implement and maintain, at its cost and expense, the technical and organisational measures:

(a) in relation to the processing of Protected Data by the Provider, as set out in and substantially in compliance with schedule 2 (*Data Processing Details*) and the Security Measures per schedule 2; and

(b) from the GDPR Date, taking into account the nature of the processing, to assist the Client insofar as is possible in the fulfilment of the Client's obligations to respond to Data Subject Requests relating to Protected Data.

2.4.2 Any additional technical and organisational measures requested by the Client shall be at the Client's cost and expense and only to the extent reasonably possible to be implemented.

2.5 Security of processing

2.5.1 The Provider shall, in respect of the Protected Data processed by it under these Terms comply with the requirements regarding security of processing set out in Data Protection Laws as applicable to Data Processors and in this Addendum including clause 2.4.

2.6 Using staff and other processors

2.6.1 Client agrees that the Provider may engage Sub-Processors to perform processing activities in respect of Personal Data on behalf of Client, as is necessary for the provision of the Dosimetry Services. The Sub-Processors currently appointed by the Provider are listed in schedule 2. The Provider will inform the Client of any addition to or change of the appointed Sub-Processors by giving no less than thirty (30) days' advance notice, and the Client will have fourteen (14) days after such notice to object to such addition or change. In the case of an objection from the Client, the Provider may choose from the following options to cure the objection:

(a) the Provider will cancel its plans to use the objectionable Sub-Processor(s) with regard to Personal Data or will offer an alternative to provide the Dosimetry Services without such Sub-Processor(s); or

(b) the Provider will take the corrective steps requested by the Client in its objection (which remove the Client's objection) and proceed to use the objectionable Sub-Processor(s) with regard to Personal Data; or

(c) the Provider may cease to provide or the Client may agree not to use (temporarily or permanently) the particular aspect of the Dosimetry Services that would involve the use of the objectionable Sub-Processor(s) with regard to Personal Data, subject to an agreement of the Provider and the Client to adjust the Fees, considering the reduced scope of the Dosimetry Services.

If none of the above options are reasonably available and the objection has not been resolved to the mutual satisfaction of the Client and Provider within 30 days after the Provider's receipt of the Client's objection, either party may terminate these Terms and the Client will be entitled to a pro-rata refund of pre-paid fees for the Dosimetry Services not performed as of the date of termination.

2.6.2 The Provider shall engage Sub-Processors under a written contract containing materially the same obligations as this clause 2, including without limitation clause 2.8 below.

2.6.3 The Provider shall take reasonable steps to ensure that all the Provider Personnel who have access to personal data are reliable and, from the GDPR Date, that all the Provider Personnel authorised to process Protected Data are subject to a binding written contractual obligation with the Provider to keep the Protected Data confidential except where disclosure is required in accordance with Applicable Law, in which case the Provider shall, where practicable and not prohibited by Applicable Law, notify the Client of any such requirement before such disclosure.

2.7 Assistance with the Client's compliance and Data Subject rights

2.7.1 The Provider shall refer all Data Subject Requests it receives to the Client within three Business Days of actual receipt of the request, and the Client shall pay the Provider reasonable expenses, as set out in the Price List, if any, for recording and referring the Data Subject Requests in accordance with this clause 2.7.1.

2.7.2 From the GDPR Date, the Provider shall provide such reasonable assistance as the Client reasonably requires, taking into account the nature of processing performed by and the information available to the Provider, to comply with the Client's obligations under Data Protection Laws with respect to the Dosimetry Services as they relate to:

(a) security of processing;

(b) DPIAs;

(c) prior consultation with a Supervisory Authority regarding high risk processing; and

(d) notifications to the Supervisory Authority and/or communications to Data Subjects by the Client in response to any Personal Data Breach,

provided the Client shall pay the Provider's Charges, per the Provider's applicable pricelist, for providing assistance under this clause 2.7.2.

2.8 International data transfers

2.8.1 The Client agrees that the Provider may transfer Protected Data outside the European Economic Area (EEA) or to any international organisation(s) (individually or collectively, an "International Recipient"), provided all transfers by the Provider of Protected Data to an International Recipient and any onward transfer shall to the extent required under Data Protection Laws be effected by way of Appropriate Safeguards and in accordance with Data Protection Laws. The foregoing sentence shall constitute Client instructions with respect to international data transfers for the purposes of clause 2.3.1.

2.8.2 The Client hereby approves the use of the Standard Contractual Clauses contained in Schedule 3 (the "Standard Contractual Clauses") as a legally enforceable mechanism for transfers of Personal Data and hereby authorises and provides a power of attorney to the Provider to enter into the Standard Contractual Clauses with the Provider in the name of and on behalf of the Client as the Data Exporter, provided that the Provider shall not modify, vary, supplement or disapply any of the Standard Contractual Clauses.

2.9 Records, information and audit

2.9.1 The Provider shall maintain, in accordance with Data Protection Laws binding on the Provider, written records of all categories of processing activities carried out on behalf of the Client.

2.9.2 The Provider shall, in accordance with Data Protection Laws, make available to the Client such information as is reasonably necessary to demonstrate the Provider's compliance with the obligations of Data Processors under Data Protection Laws, and allow for and contribute to audits, including inspections, by the Client or another auditor mandated by the Client for this purpose, subject to the Client:

(a) giving the Provider reasonable prior notice of such information request, audit or inspection being required by the Client;

(b) ensuring that all information obtained or generated by the Client or its auditor(s) in connection with such information requests, inspections and audits is kept strictly confidential, save for disclosure to the Supervisory Authority or as otherwise required by Applicable Law;

(c) ensuring that such audit or inspection is undertaken during normal business hours, with minimal disruption to the Provider's business, a Sub-Processors's business, or the business of other clients of the Provider; and

(d) paying the Provider's reasonable costs, a pre-estimate of which is set out in the Price List, for assisting with the provision of information and allowing for and contributing to inspections and audits.

2.10 Notification of Personal Data Breaches and Complaints

2.10.1 In respect of any Personal Data Breach involving Protected Data, the Provider shall, without undue delay:

(a) notify the Client of the Personal Data Breach; and

(b) provide the Client with details of the Personal Data Breach.

2.10.2 Each party shall promptly, and in any event within three Business Days, inform the other if it receives a Complaint and provide the other party with full details of such Complaint.

2.11 Deletion or return of Protected Data and copies

The Provider shall, at the Client's written request, either delete or return all the Protected Data to the Client within a reasonable time after the end of the provision of the relevant Dosimetry Services related to processing, and delete any other existing copies thereof unless storage of any data is required by Applicable Law and, where this is the case, the Provider shall inform the Client of any such requirement.

2.12 Liability, indemnities and compensation claims

2.12.1 The Client shall indemnify and keep indemnified the Provider in respect of all Data Processing Losses suffered or incurred by, awarded against or agreed to be paid by, the Provider and any Sub-Processor arising from or in connection with any:

(a) non-compliance by the Client with the Data Protection Laws;

(b) processing carried out by the Provider or any Sub-Processor pursuant to any Processing Instruction that infringes any Data Protection Law; or

(c) breach by the Client of any of its obligations under this clause 2,

except to the extent the Provider is liable under clause 2.12.2.

2.12.2 The Provider shall be liable for Data Processing Losses howsoever arising, whether in contract, tort (including negligence) or otherwise under or in connection with these Terms:

(a) only to the extent caused by the processing of Protected Data under these Terms and directly resulting from the Provider's breach of this clause 2; and

(b) in no circumstances for any portion of the Data Processing Losses (or the circumstances giving rise to them) contributed to or caused by any breach of these Terms by the Client (including a breach of clause 1.1.1(c)(ii)).

2.12.3 If a party receives a compensation claim from a person relating to processing of Protected Data, it shall promptly provide the other party with notice and full details of such claim, and each party shall:

(a) make no admission of liability nor agree to any settlement or compromise of the relevant claim without the prior written consent of the other party, which consent shall not be unreasonably withheld, conditioned or delayed; and

(b) consult fully with the other party in relation to any such action, but the terms of any settlement or compromise of the claim will be exclusively the decision of the party that is responsible under these Terms for paying the compensation.

2.12.4 The parties agree that the Client shall not be entitled to claim back from the Provider any part of any compensation paid by the Client in respect of such damage to the extent that the Client is liable to indemnify the Provider in accordance with clause 2.12.1.

2.12.5 This clause 2.12 is intended to apply to the allocation of liability for Data Processing Losses as between the parties, including with respect to compensation to Data Subjects, notwithstanding any provisions under Data Protection Laws to the contrary, except:

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

(b) that it does not affect the liability of either party to any Data Subject.

SCHEDULE 1
SECURITY MEASURES

DESCRIPTION OF TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES IMPLEMENTED BY THE PROVIDER

Technical Measures to Ensure Security of Processing	
1. Inventory and Control of Hardware Assets	Actively manage all hardware devices on the network so that only authorised devices are given access, and unauthorised and unmanaged devices are found and prevented from gaining access.
2. Inventory and Control of Software Assets	Actively manage all software on the network so that only authorised software is installed and can execute, and that unauthorised and unmanaged software is found and prevented from installation or execution.
3. Continuous Vulnerability Management	Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.
4. Controlled Use of Administrative Privileges	Maintain processes and tools to track, control, prevent, and correct the use, assignment, and configuration of administrative privileges on computers, networks, applications, and data.
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	Implement and actively manage (track, report on, correct) the security configuration of mobile devices, laptops, servers, and workstations using a configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.
6. Maintenance, Monitoring, and Analysis of Audit Logs	Collect, manage, and analyse audit and security logs of events that could help detect, understand, or recover from a possible attack.
7. Email and Web Browser Protections	Deploy automated controls to minimise the attack surface and the opportunities for attackers to manipulate human behaviour through their interaction with web browsers and email systems or content.
8. Malware Defenses	Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimising the use of automation to enable rapid updating of defense, data gathering, and corrective action.
9. Limitation and Control of Network Ports, Protocols, and Services	Manage (track, control, correct) the ongoing operational use of ports, protocols, services, and applications on networked devices in order to minimise windows of vulnerability and exposure available to attackers.

Technical Measures to Ensure Security of Processing	
10. Data Recovery Capabilities	Maintain processes and tools to properly back up personal data with a proven methodology to ensure the confidentiality, integrity, availability, and recoverability of that data.
11. Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches	Implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.
12. Boundary Defenses	Detect, prevent, and correct the flow of information transferring networks of different trust levels with a focus on personal data.
13. Data Protection	Maintain processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the confidentiality and integrity of personal data.
14. Controlled Access Based on the Need to Know	Maintain processes and tools to track, control, prevent, and correct secure access to critical or controlled assets (e.g. information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical or controlled assets based on an approved classification.
15. Wireless Access Control	Maintain processes and tools to track, control, prevent, and correct the secure use of wireless local area networks (WLANs), access points, and wireless client systems.
16. Account Monitoring and Control	Actively manage the life cycle of system and application accounts, their creation, use, dormancy, and deletion in order to minimise opportunities for unauthorised, inappropriate, or nefarious use.

Organisational Measures to Ensure Security of Processing	
17. Implement a Comprehensive Information Security Programme	Through the implementation of a Comprehensive Information Security Programme (CISP), maintain various administrative safeguards to protect personal data. These measures are designed to ensure: • security, confidentiality and integrity of personal data • protection against unauthorized access to or use of (stored) personal data in a manner that creates a substantial risk of identity theft or fraud • that employees, contractors, consultants, temporaries, and other workers who have access to personal data only process such data on instructions from the data controller.
18. Implement a Security Awareness and Training Programme	For all functional roles (prioritizing those mission critical to the business, its security, and the protection of personal data), identify the specific knowledge, skills and abilities needed to support the protection and defense of personal data; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organisational planning, training, and awareness programmes.
19. Application Software Security	Manage the security life cycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses.
20. Incident Response and Management	Protect the organisation's information, including personal data, as well as its reputation, by developing and implementing an incident response infrastructure (*e.g.*, plans, defined roles, training, communications, management oversight, retainers, and insurance) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the organisation's network and systems.
21. Security and Privacy Assessments, Penetration Tests, and Red Team Exercises	Test the overall strength of the organisation's defense (the technology, processes, and people) by simulating the objectives and actions of an attacker; as well as, assess and validate the controls, policies, and procedures of the organisation's privacy and personal data protections.
22. Physical Security and Entry Control	Require that all facilities meet the highest level of data protection standards possible, and reasonable, under the circumstances relevant to the facility and the data it contains, process, or transmits.

SCHEDULE 2

DATA PROCESSING DETAILS

1. SUBJECT-MATTER OF PROCESSING

The Provider processes Personal Data to provide Dosimetry Services for monitoring the exposure of staff of the Client, its affiliates, and their service providers and contractors who are occupationally exposed to radiation in accordance with these Terms.

2. DURATION OF THE PROCESSING

Duration of the provision of the Dosimetry Services or as per Client's instructions.

3. NATURE AND PURPOSE OF THE PROCESSING

1. The distribution and collection of personalised dosimeters;
2. The analysis, reading and recording of radiation exposure data from each dosimeter;
3. The storage of dosimeters and of data generated by dosimeters;
4. The transfer and record keeping of radiation exposure data; and
5. The reporting and provision of radiation exposure data, including to national registries as required by applicable national laws.

4. TYPE OF PERSONAL DATA

1. Name and forename, date of birth, gender (if female whether pregnant);
2. National Insurance Number (or local equivalent);
3. Occupation, facility code (type of facility employed in);
4. Current employer (name and address) and former (if available);
5. IDs and passwords for access to Landauer online system;
6. Unique dosimeter identification number;
7. Ionising radiation dose including as measured over time (dose history), including prior occupational dose history as the case may be;
8. Type of radiation intake (isotope, class and activity if radiological material were to be ingested, absorbed, inhaled and/or injected);
9. Any other personal data transferred to Provider in relation to a Data Subject, including sensitive data such as health-related information.

5. CATEGORIES OF DATA SUBJECTS

The Personal Data processed by Provider concern the following categories of Data Subjects:

1. prospective, current and former employees and contractors of the Client and its affiliates; and
2. prospective, current and former employees and contractors of the Client's service providers and contractors.

6. TECHNICAL AND ORGANIZATIONAL MEASURES

See schedule 1, which shall form a part of this schedule 2.

7. APPROVED SUB-PROCESSORS

The Agent, which promotes and sells the Dosimetry Services in certain territories, in particular UK and the Republic of Ireland, and interacts and communicates with Clients and potential clients on behalf of the Provider.

SCHEDULE 3

STANDARD CONTRACTUAL CLAUSES

EUROPEAN COMMISSION
DIRECTORATE-GENERAL JUSTICE

Directorate C: Fundamental rights and Union citizenship
Unit C.3: Data protection

Commission Decision C(2010)593
Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation: .....

Address: .....

.....

Tel.: .....; fax:.....; e-mail: .....

Other information needed to identify the organisation: .....

(the data **exporter**)

And

Name of the data importing organisation: **LANDAUER, INC.**

Address: 2 Science Road, Glenwood, Illinois, 60425, United States

Tel.: +44 (0) 1865 373 008; fax: +44 (0) 1865 373 017; e-mail: admin@landauer.co.uk

(the data **importer**)

each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1
Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) '*the data exporter*' means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law*' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2
Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3
Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4
Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6
Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7
Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established, namely the laws of England and Wales.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.
2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established, namely .....
4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

This agreement is dated: ……

On behalf of the data exporter:

Name: …….

represented by its duly authorised attorney **LANDAUER, INC., Bertrand Sérisé**, VP Sales, EMEA

Position: VP Sales, EMEA

Address: 2 Science Road, Glenwood, Illinois, 60425, United States

Other information necessary in order for the contract to be binding (if any):

Signature…….

On behalf of the data importer: LANDAUER, INC.

Name: **Bertrand Sérisé**

Position: VP Sales, EMEA

Address: 2 Science Road, Glenwood, Illinois, 60425, United States

Other information necessary in order for the contract to be binding (if any):

Signature…….

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter

The data exporter employs personnel who in the course of their employment may be exposed to radiation and such exposure needs to be constantly monitored in accordance with regulations governing exposure to ionising radiation.

Data importer

The data importer is a provider of personnel dosimetry monitoring services approved by the relevant health and safety regulator.

Data subjects

The Personal Data processed by Provider concern the following categories of Data Subjects:

(i) prospective, current and former employees and contractors of the Client and its affiliates; and

(ii) prospective, current and former employees and contractors of the Client's service providers and contractors.

Categories of data

The personal data transferred concern the following categories of data

1. Name and forename, date of birth, gender (if female whether pregnant);
2. National Insurance Number (or local equivalent);
3. Occupation, facility code (type of facility employed in);
4. Current employer (name and address) and former (if available);
5. IDs and passwords for access to Landauer online system;
6. Unique dosimeter identification number;

Special categories of data (if appropriate)

7. Ionising radiation dose including as measured over time (dose history), including pior occupational dose history as the case may be;
8. Type of radiation intake (isotope, class and activity if radiological material were to be ingested, absorbed, inhaled and/or injected);
9. Any other sensitive data including health-related information.

Processing operations

The personal data transferred will be subject to the following basic processing activities:

1. The distribution and collection of personalised dosimeters;
2. The analysis, reading and recording of radiation exposure data from each dosimeter;
3. The storage of dosimeters and of data generated by dosimeters;
4. The transfer and record keeping of radiation exposure data; and
5. The reporting and provision of radiation exposure data, including to national registries as required by applicable national laws.

DATA EXPORTER
Name: …….
represented by its duly authorised attorney LANDAUER, INC., Bertrand Sérisé, VP Sales, EMEA

Authorised Signature ……

DATA IMPORTER
Name: LANDAUER, INC., Bertrand Sérisé, VP Sales, EMEA

Authorised Signature ……

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

Technical Measures to Ensure Security of Processing	
1. Inventory and Control of Hardware Assets	Actively manage all hardware devices on the network so that only authorised devices are given access, and unauthorised and unmanaged devices are found and prevented from gaining access.
2. Inventory and Control of Software Assets	Actively manage all software on the network so that only authorised software is installed and can execute, and that unauthorised and unmanaged software is found and prevented from installation or execution.
3. Continuous Vulnerability Management	Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.
4. Controlled Use of Administrative Privileges	Maintain processes and tools to track, control, prevent, and correct the use, assignment, and configuration of administrative privileges on computers, networks, applications, and data.
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	Implement and actively manage (track, report on, correct) the security configuration of mobile devices, laptops, servers, and workstations using a configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.
6. Maintenance, Monitoring, and Analysis of Audit Logs	Collect, manage, and analyse audit and security logs of events that could help detect, understand, or recover from a possible attack.
7. Email and Web Browser Protections	Deploy automated controls to minimise the attack surface and the opportunities for attackers to manipulate human behaviour through their interaction with web browsers and email systems or content.
8. Malware Defenses	Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimising the use of automation to enable rapid updating of defense, data gathering, and corrective action.
9. Limitation and Control of Network Ports, Protocols, and Services	Manage (track, control, correct) the ongoing operational use of ports, protocols, services, and applications on networked devices in order to minimise windows of vulnerability and exposure available to attackers.
10. Data Recovery Capabilities	Maintain processes and tools to properly back up personal data with a proven methodology to ensure the confidentiality, integrity, availability, and recoverability of that data.
11. Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches	Implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.
12. Boundary Defenses	Detect, prevent, and correct the flow of information transferring networks of different trust levels with a focus on personal data.

Technical Measures to Ensure Security of Processing	
13. Data Protection	Maintain processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the confidentiality and integrity of personal data.
14. Controlled Access Based on the Need to Know	Maintain processes and tools to track, control, prevent, and correct secure access to critical or controlled assets (e.g. information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical or controlled assets based on an approved classification.
15. Wireless Access Control	Maintain processes and tools to track, control, prevent, and correct the secure use of wireless local area networks (WLANs), access points, and wireless client systems.
16. Account Monitoring and Control	Actively manage the life cycle of system and application accounts, their creation, use, dormancy, and deletion in order to minimise opportunities for unauthorised, inappropriate, or nefarious use.

Organisational Measures to Ensure Security of Processing	
17. Implement a Comprehensive Information Security Programme	Through the implementation of a Comprehensive Information Security Programme (CISP), maintain various administrative safeguards to protect personal data. These measures are designed to ensure: • security, confidentiality and integrity of personal data • protection against unauthorized access to or use of (stored) personal data in a manner that creates a substantial risk of identity theft or fraud • that employees, contractors, consultants, temporaries, and other workers who have access to personal data only process such data on instructions from the data controller.
18. Implement a Security Awareness and Training Programme	For all functional roles (prioritizing those mission critical to the business, its security, and the protection of personal data), identify the specific knowledge, skills and abilities needed to support the protection and defense of personal data; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organisational planning, training, and awareness programmes.
19. Application Software Security	Manage the security life cycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses.
20. Incident Response and Management	Protect the organisation's information, including personal data, as well as its reputation, by developing and implementing an incident response infrastructure (*e.g.*, plans, defined roles, training, communications, management oversight, retainers, and insurance) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the organisation's network and systems.
21. Security and Privacy Assessments, Penetration Tests, and Red Team Exercises	Test the overall strength of the organisation's defense (the technology, processes, and people) by simulating the objectives and actions of an attacker; as well as, assess and validate the controls, policies, and procedures of the organisation's privacy and personal data protections.
22. Physical Security and Entry Control	Require that all facilities meet the highest level of data protection standards possible, and reasonable, under the circumstances relevant to the facility and the data it contains, process, or transmits.

DATA EXPORTER
Name: …….
represented by its duly authorised attorney LANDAUER, INC., Bertrand Sérisé, VP Sales, EMEA

Authorised Signature ……

DATA IMPORTER
Name: LANDAUER, INC., Bertrand Sérisé, VP Sales, EMEA

Authorised Signature ……