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:

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

"**Provider**" means LANDAUER NORDIC HOLDINGS AB, a company incorporated in Sweden, having its registered address at Uggledalsvägen 29, SE 427 40 Billdal, Sweden, 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 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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 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;

"**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 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 Protected 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; and

(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.

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 schedule2 (*Data Processing Details*) and the Security Measures per schedule 1; and

(b) 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 Protected 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:

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

(d) 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 Protected Data; or

(e) 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 Protected 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 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 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 Provider may not transfer any Protected Data to any country or territory outside the European Economic Area (EEA) or to any international organisation(s) (individually or collectively, an "International Recipient"), without first obtaining the general or express written consent of Customer and, if Customer consents to the transfer of Protected Data to an International Recipient, Provider shall ensure that such transfer and any onward transfer to any recipient thereafter: (a) is effected by way of Appropriate Safeguards; (b) complies with Clause 2.3.1 above; and (c) otherwise complies with Data Protection Laws.

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.

PROVIDER

Name: ……

represented by ……, Director

Signature …… Date: ……..

CLIENT

Name: ……

represented by ……, Title: ……

Signature …… Date: ……..

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.
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 administration of subscriptions and purchase orders for dosimetry monitoring services, including invoicing;
2. The manufacturing, distribution and supply of dosimeters;
3. The analysis and reading-out of dosimeters;
4. The reporting and provision of radiation exposure data, including to national registries as required by applicable national laws.

4. TYPE OF PERSONAL DATA

1. First and last name, sex, date of birth, contact details and/or professional (email, telephone, address);
2. Employer (Client: name, company id number, address);
3. Occupation, facility code (type of facility employed in);
4. National Insurance Number;
5. Exposure data (doses and wear periods, organs or tissue exposed);
6. 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

1. Within the European Economic Area (EEA)
    a. LANDAUER EUROPE, SAS, 9, rue Paul Dautier, Vélizy-Villacoublay, 78140, France
        i. An affiliated company of Provider
        ii. Activities
            1. Manufacturing of dosimeters ;
            2. Analysis and reading-out of extremity, lens of eye and neutron dosimeters.