THIS "GDPR" APPENDIX IS AN INTEGRAL PART OF THE DOSIMETRIC MONITORING CONTRACT ESTABLISHED BETWEEN THE CUSTOMER AND THE SUPPLIER IN THE SAME WAY AS THE GENERAL CONDITIONS OF SALE TRAINING

1. DEFINITIONS AND INTERPRETATION

1.1 Definitions

" **Supplier** " means LANDAUER EUROPE SAS;

" **Services** " means the dosimetric monitoring and radiation protection training services covered by the Contracts;

" **Appropriate Guarantees** " means the legally applicable mechanism(s) relating to the transfer of Personal Data as authorized under the " Computer Regulations and Freedoms " defined below ;

" **Applicable Law** " means the law applicable to the Contract;

" **Data Processing Losses** " means all of the following liabilities and amounts:

(a) costs (including legal costs), claims, demands, legal actions, settlements, charges, proceedings, 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 of a Data Holder by a Supervisory Authority; And

(iii) reasonable costs of responding to and complying with investigations carried out by a Supervisory Authority;

" **Computer regulations and freedoms** " means the following texts, applicable and binding for the Customer, the Supplier, or the Services :

(a) In France :

(i) Law No. 75-17 of January 6, 1978 relating to data processing, files and freedoms (the " **Informatics and freedoms law** ") as well as any law or regulation implementing the Council of Europe Directives 95/46/ EC (the " **Data Protection Directive** ") or 2002/58/EC (the " **Privacy and Electronic Communications Directive** "); and or

(ii) the Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) ("GDPR") **,** repealing Directive 95/46/EC, and/or any corresponding or equivalent national law or regulation (the " **amended Data Protection Act** ");

(b) in other countries of the European Union: the GDPR and all laws or regulations of the Member States giving effect to or corresponding to the later;

"**Request from the data subject** " means a request, by any Data Subject, to exercise any right available to them under the Data Protection Regulations. ;

" **Complaint** " means a grievance or request relating to the obligations of a party under the Data Protection Regulations which concern this contract. This term includes requests for compensation made by a Data Subject as well as any advice, investigation or other action taken by a Supervisory Authority;

" **EIVP** " means a data protection impact assessment under the Data Protection Laws;

LANDAUER
9, rue Paul Dautier - CS 60731
78457 Vélizy-Villacoublay Cedex
FRANCE

Tel. +33 (0)1 40 95 62 90
Email service@landauer.fr
Web www.landauer.fr

Au capital de 3.446.950 euros
441 462 033 RCS Versailles - APE 7112B
N° TVA : FR 06 441 462 033

" **GDPR Date** " means the date from which the GDPR applies, namely May 25, 2018;

" **Personal Data Breach** " means any security breach resulting in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data;

" **Protected Data** " means Personal Data received from or on behalf of the Customer in connection with the performance of the Supplier's obligations under this Agreement;

" **Second-tier Subcontractor** " means another Subcontractor engaged by the Supplier to carry out Protected Data processing activities on behalf of the Customer;

" **Controlling authority** " means any agency, department, official manager, parliament, public or regulatory body as well as any government or professional body, regulatory authority or supervisory authority responsible for the implementation and control of the Data Protection Regulations . ;

1.2 Interpretation

In this contract:

1.2.1 The terms " **Data Controller** " (or "File Controller"), " **Subcontractor** ", " **Data Subjects** ", " **international organization** ", " **Personal Data** " and " **processing** " meet the definitions given in the Data Protection Laws.

1.2.2 references to the Data Protection Act or the Data Protection Directive and to the terms defined therein must be replaced by or integrate (where applicable) references to any Applicable Law replacing, modifying, extending, bringing into force or consolidating said Applicable Law (including in particular the GDPR) as well as the equivalent terms defined in said Applicable Law, once the latter comes into force;

1.2.3 to the extent that a clause of this contract requires the execution by a party of an obligation "in accordance with the Data Protection Regulations " (or similar), unless otherwise expressly agreed in this contract, the latter requires execution in accordance with the relevant provisions of the said Data Protection Regulations in force and applicable at the time of execution (if applicable) ;

---

2. DATA PROTECTION

2.1 Subcontractor/Processing Controller

2.1.1 The parties agree that, for Protected Data, the Customer is the Data Controller and that the Supplier is the Processor of the Protected Data.

2.1.2 In the event that the Customer is not the Data Controller but a Subcontractor of rank n, the Supplier acts as a Subcontractor of rank n+1. The clauses described below apply in the same way.

2.2 Compliance with IT Regulations and freedoms and obligations of the parties

2.2.1 The Supplier must process Protected Data in accordance with:

(a) the obligations of Subcontractors under the IT Regulations and freedoms relating to the performance of its obligations under this Contract, and

(b) all of the conditions of this Contract;

2.2.2 The Customer must comply with :

(a) IT Regulations and freedoms relating to the processing of Protected Data, the Services and the exercise and execution of its respective rights and obligations under this Agreement, including

LANDAUER
9, rue Paul Dautier - CS 60731
78457 Vélizy-Villacoublay Cedex
FRANCE
Tel. +33 (0)1 40 95 62 90
Email service@landauer.fr
Web www.landauer.fr

Au capital de 3.446.950 euros
441 462 033 RCS Versailles - APE 7112B
N° TVA : FR 06 441 462 033

maintaining all relevant regulatory formalities and declarations in accordance with the IT Regulations and freedoms ; And

(b) all of the conditions of this Contract;

2.2.3 The Customer guarantees, declares and undertakes to the following elements:

(a) the data transmitted to the Supplier for the provision of the Services under this Contract must have been provided by the Client in all respects in accordance with the Data Protection Regulations , including in terms of collection, storage and processing, which, for the avoidance of doubt, includes the Client providing all required fair processing information and obtaining all necessary consents from Data Subjects;

(b) all instructions given by him to the Supplier relating to Personal Data must always be in accordance with the Data Protection Regulations;

(c) he has demonstrated reasonable diligence with regard to the Supplier's processing operations, and he is convinced that:

(i) the Supplier's processing operations are suitable for the purposes for which the Customer wishes to use the Services and has engaged the Supplier to ensure the processing of Protected Data; And

(ii) the Supplier has sufficient expertise, reliability and resources to implement all technical and organizational measures meeting the requirements of the IT and Freedoms Regulations.

2.2.4 The Customer may not withhold, delay or unreasonably condition its acceptance of any changes requested by the Supplier for the purpose of ensuring that the Services and the Supplier (or any second-tier Subcontractor) comply with the Protection Laws of Data, and in any case not more than 1 month.

2.3 Details of data processing and related instructions

2.3.1 To the extent that the Supplier processes Protected Data on behalf of the Customer, the Supplier:

(a) unless otherwise required by Applicable Law, is required (and must ensure that any person acting under its authority is required) to process Protected Data in strict accordance with the Customer's written and documented instructions as set out in the present [article 2] as well as in [appendix 2 and 3] (Details of Data Processing), possibly updated;

(b) is required, if an Applicable Law requires it to process Protected Data other than in accordance with the Data Processing Instructions, to inform the Customer of such requirement before any processing of the Protected Data (unless the Applicable Law prohibits it from doing so for reasons of major public interest); And

(c) is required to inform the Client if an Instruction, in his opinion, infringes the Data Protection Regulations:

(i) provided that this is without prejudice to [articles 2.2.2 and 2.2.3];

(ii) provided that, to the fullest extent permitted by applicable law, Supplier shall have no liability whatsoever (whether in contract, tort, including negligence, or otherwise) for any loss, cost, expense or liability (including any Data Processing Loss) arising out of or in connection with any processing carried out in accordance with the Customer's

LANDAUER
9, rue Paul Dautier - CS 60731
78457 Vélizy-Villacoublay Cedex
FRANCE
Tel. +33 (0)1 40 95 62 90
Email service@landauer.fr
Web www.landauer.fr

Processing Instructions after the Supplier has informed the Customer of an infringing Data Processing Instruction; And

(iii) it being understood that this [article 2.3.1 (c)] will only apply from the GDPR Date.

2.3.2 The processing of Protected Data carried out by the Supplier under this Contract includes the processing activities indicated in [appendix 2 and 3] (*Details of Data Processing*) as regularly updated.

2.4 Technical and organizational measures

2.4.1 The Supplier is required to implement and maintain, at its own expense, the technical and organizational measures:

(a) regarding the processing of Protected Data by the Supplier, as set out in [appendix 2 and 3] (*Details of Data Processing*), and the various Security Measures agreed and described in [appendix 1]; And

(b) from the GDPR Date, taking into account the nature of the processing, to assist the Client, to the extent possible, in fulfilling its obligations to respond to Requests from Data Subjects relating to Protected Data.

2.4.2 All additional technical and organizational measures requested by the Customer will be taken at the expense and expense of the latter, and only to the extent possible.

2.5 Securing Data Processing

2.5.1 The Supplier must, for all Protected Data processed under this contract, comply with all the requirements relating to the security of processing imposed by the Data Protection Regulations and by this Contract, including [article 2.4].

2.6 Second-Level Subcontractors

2.6.1 The Customer authorizes the Supplier to engage second-tier subcontractors to carry out processing activities relating to the Customer's Personal Data on its behalf, or to transfer or disclose the Customer's Personal Data to any third party if a such action is necessary for the provision of the Services. The Client approves the second level Subcontractors indicated in [appendix 2 and 3]. The Supplier will inform the Customer of any change in second-level Subcontractor, the Customer then having 1 month to raise objections against this change.

2.6.2 The Supplier will engage said second-level Subcontractors, who present sufficient guarantees to guarantee the protection of the Customer's Personal Data, within the framework of written contracts containing the same obligations as this [article 2] and including, without limitation limit thereto, [article 2.8] below.

2.6.3 The Supplier must take all reasonable measures to ensure that all members of the Supplier's personnel with access to the Protected Data are reliable and, as of the GDPR Date; that all members of the Supplier's personnel authorized to process the Protected Data are bound by a contractual obligation to guarantee the confidentiality of the Protected Data (except where disclosure of the latter is required by any Applicable Law, in which case the Supplier must, (if practically possible and not prohibited by such Applicable Law, inform Customer of such obligation prior to any disclosure).

LANDAUER
9, rue Paul Dautier - CS 60731
78457 Vélizy-Villacoublay Cedex
FRANCE
Tel. +33 (0)1 40 95 62 90
Email service@landauer.fr
Web www.landauer.fr

2.7 Assistance with Customer Compliance Efforts and Data Holder Rights

2.7.1 Supplier must transmit to Customer all Data Subject Requests it receives within three business days of receipt, and Customer will pay the costs of recording and forwarding such requests at Supplier's applicable rate.

2.7.2 From the date of the GDPR, the Supplier will provide all reasonable assistance that the Customer may require, taking into account the nature of the processing carried out and the information available to the Supplier, to comply with the Customer's obligations in under the IT and freedoms regulations relating to the Services when they concern:

(a) securing data processing;

(b) EIVPs;

(c) before any consultation with a Supervisory Authority regarding high-risk processing; And

(d) any notice sent to a Supervisory Authority and/or any communication to Data Subjects in response to a possible violation of Personal Data;

to the extent that the Customer will pay the Supplier's costs, according to its applicable rate, relating to the provision of said assistance under this Agreement [article 2.7.2]

2.8 International data transfers

2.8.1 The Supplier will not transfer any Personal Data of the Customer to a country or territory located outside the European Economic Area, nor to any international organization, and will not allow any of its Subcontractors to do so.

2.9 Register, information and audit

2.9.1 The Supplier must keep, in accordance with the Data Protection Regulations , written records of all categories of processing activities carried out on behalf of its Clients.

2.9.2 The Supplier must, in accordance with the Data Protection Regulations , make available to the Customer the information reasonably necessary to demonstrate compliance with its obligations as a Subcontractor under the Data Protection Regulations . The Supplier must further enable and contribute to audits, which may include inspections, carried out by the Customer or by another auditor mandated by the Customer for this purpose, provided that the Customer:

(a) gives the Supplier reasonable notice of any such request for information, audit or inspection;

(b) ensures that all information obtained or generated by the Client or its auditor in the context of such requests for information, inspection or audit remains strictly confidential, with the exception of possible disclosure to the Authority control or as required by Applicable Law;

(c) ensures that such an audit or inspection is undertaken during normal business hours, with minimal disruption to the activities of the Supplier, its second-tier Subcontractors, and other customers of the Supplier; And

(d) shall pay to Supplier the costs incurred in assisting in providing such information and enabling and contributing to such inspections and audits, at Supplier's applicable rate.

2.10 Personal Data Breach Notices and Complaints

2.10.1 In the event of a Personal Data Breach, the Supplier must, as soon as possible :

(a) inform the Customer of such a Personal Data breach; And

LANDAUER
9, rue Paul Dautier - CS 60731
78457 Vélizy-Villacoublay Cedex
FRANCE
Tel. +33 (0)1 40 95 62 90
Email service@landauer.fr
Web www.landauer.fr

Au capital de 3.446.950 euros
441 462 033 RCS Versailles - APE 7112B
N° TVA : FR 06 441 462 033

(b) provide the Customer with details of the Personal Data breach.

2.10.2 Each party must promptly and in any event within three business days notify the other party if it receives a Claim, providing the other party with all related details.

2.11 Deletion or return of Protected Data and copies thereof

2.11.1 Supplier shall, upon Customer's written request, delete or return all Protected Data to Customer within a reasonable time after completion of the provision of the Data Processing Services , and delete any other existing copies thereof unless storage data is required by Applicable Law. Where applicable, The Supplier informs the Customer of the existence of such requirements.

2.11.2 The Customer will pay the Supplier any costs according to its applicable rate.

2.12 Liability, Indemnity and Claims

2.12.1 The Customer indemnifies the Supplier in the event of damage suffered as a result of or in connection with:

(a) non-compliance by the Customer with IT Regulations and freedoms ;

(b) any processing carried out by the Supplier or any second-level Subcontractor in accordance with any Processing Instruction which violates the Data Protection Regulations; Or

(c) the violation by the Customer of any of its obligations under this [article 2];

except to the extent that the Supplier's liability is committed under [article 2.12.2].

2.12.2 Supplier will be liable for Losses in Data Processing, however caused, whether such liability is in contract, tort (including negligence) or otherwise under or in connection with this Agreement:

(a) solely in relation to the Processing of Protected Data under this Agreement and resulting directly from a breach of this [section 2] by the Supplier; And

(b) in no case for any part or all of the Losses in Data Processing (or for the circumstances giving rise thereto) caused by a breach of this Agreement by the Customer (and including a breach of [section 2.3.1 (c) (ii)]).

2.12.3 If a party receives a third party compensation claim related to the Processing of Protected Data, it must promptly notify the other party with full details of the claim.

(a) The parties are not authorized in any such circumstance to admit any liability or agree to any settlement or compromise without the prior written consent of the other party, which consent shall not be unduly withheld, conditioned or delayed; And

(b) Each party must consult fully with the other party regarding any such action. However, the terms of any possible settlement or compromise will be exclusively the decision of the party responsible, under this Contract, for the payment of compensation.

2.12.4 The parties agree that the Customer does not have the right to claim from the Supplier any part or all of any compensation paid by the Customer for the damages mentioned above to the extent that the Customer is required to compensate the Supplier in accordance with [article 2.12.1].

2.12.5 This [article 2.12] concerns the attribution of responsibilities between the parties in the event of Losses in the Processing of Data, which includes the compensation of the Persons concerned, notwithstanding any provision contrary to the Data Protection Regulations ;

(a) to the extent authorized by Applicable Laws (including the Data Protection Regulations); And

(b) to the extent that the liability of the parties to a Data Subject is not affected by its provisions.

LANDAUER
9, rue Paul Dautier - CS 60731
78457 Vélizy-Villacoublay Cedex
FRANCE
Tel. +33 (0)1 40 95 62 90
Email service@landauer.fr
Web www.landauer.fr

APPENDIX 1

SECURITY MEASURES

DESCRIPTION OF THE TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES IMPLEMENTED BY LANDAUER EUROPE SAS

Technical measures to ensure the safety of processing	
1. Inventory and control of material resources	Actively manage all hardware devices on the network so that only authorized devices have access, and unauthorized and unmanaged devices are detected and prevented from accessing them.
2. Inventory and control of software resources	Actively manage all software on the network so that only authorized software is installed and can be run, and unauthorized and unmanaged software is identified and prevented from being installed or run.
3. Permanent monitoring of new vulnerabilities	Monitor and evaluate any new Cyber Security information and take appropriate measures to identify vulnerabilities, correct and minimize the window of opportunity for attackers.
4. Controlled use of administrative privileges	Manage 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 of hardware and software on mobile devices, laptops, workstations and servers	Actively implement and manage (track, report, remediate) security configuration of mobile devices, laptops, servers and workstations using a configuration management and change control process to prevent malicious exploitation of services and vulnerable parameters.
6. Maintenance, monitoring and analysis of audit logs	Collect, manage and analyze audit and security logs of events that could help detect, understand or repair after a possible attack.
7. Email Protection and Web Browsing	Deploy automated controls to minimize the scope of an attack and the opportunities for attackers to manipulate human behavior through their interaction with web browsers and email systems or its content.

LANDAUER
9, rue Paul Dautier - CS 60731
78457 Vélizy-Villacoublay Cedex
FRANCE

Tel. +33 (0)1 40 95 62 90
Email service@landauer.fr
Web www.landauer.fr

Au capital de 3.446.950 euros
441 462 033 RCS Versailles - APE 7112B
N° TVA : FR 06 441 462 033

Technical measures to ensure the safety of processing	
8. Defense against computer viruses	Control the installation, spread and execution of malicious code across multiple locations across the enterprise, while optimizing the use of automation to enable rapid updating of defenses, data collection and management. 'corrective action.
9. Limitation and control of network ports, protocols and services	Supervise (track, control, correct) the use of ports, protocols, services and applications on networked equipment to minimize windows of vulnerability and exposure available to attackers.
10. Data Recovery Capabilities	Maintain personal data backup processes and tools with a proven methodology to ensure the confidentiality, integrity, availability and recovery of this data.
11. Secure configuration for network devices, such as firewalls, routers and switches	Actively implement and manage (track, report, remediate) security configuration of network infrastructure devices using a configuration management and change control process to prevent hackers from exploiting services and vulnerable parameters.
12. Network partitioning _	Detect and prevent information flows between networks of different trust levels with a focus on personal data.
13. Data protection	Maintain the processes and tools used to prevent data exfiltration, reduce the impact of exfiltrated data, and ensure the confidentiality and integrity of personal data.
14. Limitation of access according to need	Maintain processes and tools to track, control, prevent, and remediate secure access to critical or controlled resources (e.g., information, resources, systems) based on formal determination of people, computers, and applications having a need and right of access to these critical or controlled resources according to an approved classification.
15. Wireless Access Control	Manage processes and tools to track, control, prevent and remediate the secure use of wireless local area networks (WLANs), access points and wireless client systems.
16. Monitoring and control of accounts	Actively manage the lifecycle of system and application accounts, their creation, use, inactivity and deletion to minimize opportunities for unauthorized or inappropriate use

LANDAUER
9, rue Paul Dautier - CS 60731
78457 Vélizy-Villacoublay Cedex
FRANCE
Tel. +33 (0)1 40 95 62 90
Email service@landauer.fr
Web www.landauer.fr

Au capital de 3.446.950 euros
441 462 033 RCS Versailles - APE 7112B
N° TVA : FR 06 441 462 033

Organizational measures to ensure the security of processing	
17. Implement a comprehensive IT security program	Through the implementation of a comprehensive information security program (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 way that presents a significant risk of identity theft or fraud • that employees, contractors, consultants, temporary workers and other parties who have access to personal data only process such data on the instructions of the data controller.
18. Implement a security awareness and training program	For each function in the organization (priority critical missions to the activity, its security and the protection of personal data), identify the specific knowledge, skills and abilities necessary for employees to ensure the protection and defense of data personal; develop and deploy an integrated plan to assess, identify and remedy problems by applying procedures, organizational planning, training and awareness actions.
19. Software Security _ applications	Manage the security lifecycle of all internally developed and acquired software to prevent, detect and remediate security vulnerabilities.
20. Incident response and management	Protect the organization's information, including personal data, as well as its reputation, by developing and implementing an incident response infrastructure (e.g. plans, defined roles, training, communication, management oversight, retention and insurance) to quickly detect an attack and effectively contain the damage, eradicate the attacker's presence and restore the integrity of the organization's network and systems.
21. Security and confidentiality assessment, information system penetration testing	Test the robustness of the organization's means of protection (technology, processes and people) by simulating the objectives and actions of an attacker; assess and validate the organization's existing controls, policies and procedures for protecting confidentiality and personal data.
22. Physical security and access control to facilities	Obtain that all facilities meet the highest data protection standards reasonably practicable, taking into account the context of each facility and the data it contains, processes or transmits.

LANDAUER
9, rue Paul Dautier - CS 60731
78457 Vélizy-Villacoublay Cedex
FRANCE
Tel. +33 (0)1 40 95 62 90
Email service@landauer.fr
Web www.landauer.fr

Au capital de 3.446.950 euros
441 462 033 RCS Versailles - APE 7112B
N° TVA : FR 06 441 462 033

APPENDIX 2

DETAILS OF DATA PROCESSING FOR DOSIMETRIC MONITORING

1. PURPOSE OF TREATMENT

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 TREATMENT

Duration of the contract, and according to the Client's Instructions.

3. NATURE AND PURPOSE OF THE PROCESSING

1. Administration of dosimetric monitoring subscriptions/orders;
2. Supply of dosimeters;
3. Analysis of dosimeters;
4. Communication of results, including national dose register if applicable;
5. Billing.

4. TYPES OF PERSONAL DATA

1. Name, first name, gender, date of birth, personal and/or professional contact details (email, telephone, address);
2. Employer (Client: company name, Business registration number, address);
3. Sector of activity and profession, classification of the worker in terms of radiation protection (A, B);
4. Registration in the national security system (such as RNIPP, NIN, SSN);
5. Internal customer number
6. Occupational doctor (last name, first name, address of the occupational doctor);
7. Information relating to exposure (doses and integration period, exposed organs or tissues).

5. CATEGORIES OF PEOPLE CONCERNED

Workers likely to be exposed to ionizing radiation.

6. TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

See [Appendix 1], which forms part of this [Appendix 2]

7. -TIER SUBCONTRACTORS APPROVED AND PROCESSING ACTIVITIES ASSIGNED

1. esi in Saint-Priest (France), for the printing and routing of certain paper documents.
2. La Poste/DPD (France) for the distribution of dosimeters
3. Ciblex (France), for the distribution of dosimeters
4. Chronopost (France) for the distribution of dosimeters
5. DHL (France) for the distribution of dosimeters
6. DataBank (France) for data hosting
7. DocuWare (France) for editing and archiving reports

LANDAUER
9, rue Paul Dautier - CS 60731
78457 Vélizy-Villacoublay Cedex
FRANCE

Tel. +33 (0)1 40 95 62 90
Email service@landauer.fr
Web www.landauer.fr

Au capital de 3.446.950 euros
441 462 033 RCS Versailles - APE 7112B
N° TVA : FR 06 441 462 033

APPENDIX 3

DETAILS OF DATA PROCESSING FOR TRAINING

1. PURPOSE OF TREATMENT

RADIATION PROTECTION TRAINING FOR WORKERS LIKELY TO BE EXPOSED TO IONIZING RADIATION

In France, according to the following regulatory framework:

1. Decree No. 2023-489 of June 21, 2023 relating to the protection of workers against the risks due to ionizing radiation amending Decree No. 2003-296 of March 31, 2003 relating to the protection of workers against the dangers of ionizing radiation;
2. Decision no. 2017-DC-0585 of March 14, 2017 modified by Decision no. 2019-DC-0669 of the ASN of June 11, 2019 referring to the Educational Guides related to training in the radiation protection of exposed persons

2. DURATION OF TREATMENT

Duration of the contract, and according to the Client's Instructions.

3. NATURE AND PURPOSE OF THE PROCESSING

1. Management of training requests
2. Communication of training certificates
3. Storage of training certificates
4. Billing.

4. TYPES OF PERSONAL DATA

1. Name, first name, email
2. Employer (Client: company name, Business registration number, address);
3. Sector of activity and profession,

5. CATEGORIES OF PEOPLE CONCERNED

Workers likely to be exposed to ionizing radiation.

6. TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

See [Appendix 1], which forms part of this [Appendix 3]

7. SECOND-TIER SUBCONTRACTORS APPROVED AND PROCESSING ACTIVITIES ASSIGNED

C2i santé in Maxeville (France) for the provision of the online Radioprotection training platform and possible invoicing

LANDAUER
9, rue Paul Dautier - CS 60731
78457 Vélizy-Villacoublay Cedex
FRANCE
Tel. +33 (0)1 40 95 62 90
Email service@landauer.fr
Web www.landauer.fr

Au capital de 3.446.950 euros
441 462 033 RCS Versailles - APE 7112B
N° TVA : FR 06 441 462 033