Data Processing Addendum ("**Agreement**")

BETWEEN

(1) **Mirion Technologies (Dosimetry Services) B.V.,** incorporated and registered in the Netherlands with company number 718 754 76 whose registered office is at Utrechtseweg 310 – B54, 6812 AR Arnhem, The Netherlands with mailing address Utrechtseweg 310 – B54, 6812 AR Arnhem, The Netherlands ("**Mirion**");

– OR –

Mirion Technologies (AWST) GmbH, registered at the District Court of Munich, Germany, under no. HRB 250417 whose registered office is at Otto-Hahn-Ring 6, DE-81739, München, Germany with mailing address Otto-Hahn-Ring 6, DE-81739, München, Germany ("**Mirion**");

– OR –

Mirion Technologies (GDS), Inc., incorporated and registered in Delaware with company number 3700491 whose registered office is at c/o Cogency Global Inc., 850 New Burton Road, Ste 201, Dover, DE 19904 USA with mailing address 104 Union Valley Road, Oak Ridge, TN 37830, USA ("**Mirion**")

and

(2) The legal entity that is party to and executed the underlying Services Agreement as a Customer or the underlying Distributor Agreement as a Distributor (the "**Customer**").

BACKGROUND

(A) Mirion provides monitoring of individuals for occupational exposure to ionizing radiation and related services ("**Services**") to the Customer pursuant to an agreement ("**Services Agreement**").

(B) This Agreement forms part of and is incorporated by reference into the Services Agreement entered into by the Customer and Mirion concerning Customer's use of the Services to reflect the parties' agreement regarding the Processing of Personal Data in accordance with Data Protection Legislation and sets out the framework for the transferring of Personal Data from the Customer to Mirion to be processed for the purpose of providing the Services.

(C) This Agreement consists of the terms described herein, Schedule 1, Schedule 2 and Schedule 3 including any Attachments thereto. By executing the Services Agreement, the parties are agreeing to all parts of this Agreement.

1 Definitions

1.1 In this Agreement

1.1.1 "**Affiliate**" means an entity that directly or indirectly Controls, is Controlled by or is under common Control with an entity. "Control" means an ownership, voting or similar interest representing fifty percent (50%) or more of the total interests then outstanding of the entity in question. The term "Controlled" will be construed accordingly;

1.1.2 "**Customer Personal Data**" means any Customer Data that is personal data that Mirion processes on behalf of Customer in the course of providing the Services;

1.1.3 "**Data Protection Legislation**" shall mean one or more of the following as may be applicable to the Personal Data Processed by Mirion on behalf of the Customer in its provision of the Services: Data Protection Act 2018 (UK), General Data Protection Regulation ("**GDPR**") means: (i) where applicable the General Data Protection Regulation (EU) 2016/679 ("**EU GDPR**"); (ii) where applicable the EU GDPR as implemented into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 (the "**UK GDPR**"), the Swiss Federal Act on Data Protection ("**FADP**"), and in each case shall include any equivalent legislation in such jurisdictions which shall apply to Processing of Personal Data, in each case as amended, extended or re-enacted from time to time and all orders, regulations, statutes, instruments or other subordinate legislation made thereunder in the European Union ("**EU**"), the European

Economic Area ("**EEA**") and their member states, Switzerland and the United Kingdom ("**UK**") from time to time;

1.1.4 "**Data Subject**", "**Controller**", "**International Organisation**", "**Processor**" and "**Processing**" have the same meaning as in the Data Protection Legislation;

1.1.5 "**Personal Data**" has the meaning set out in the Data Protection Legislation;

1.1.6 "**Restricted Transfer**" means: (i) where the EU GDPR applies, a transfer of personal data from the European Economic Area to a country outside of the European Economic Area which is not subject to an adequacy decision by the European Commission; (ii) where the UK GDPR applies, a transfer of personal data from the United Kingdom to any other country which is not based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018; and (iii) where the FADP applies, a transfer of personal data to a country outside of Switzerland which is not included on the list of adequate jurisdictions published by the Swiss Federal Data Protection and Information Commissioner;

1.1.7 "**Standard Contractual Clauses**" shall mean where the EU GDPR applies, the standard contractual clauses adopted by the European Commission pursuant to Commission Decision C/2021/3972 for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council ("**EU Standard Contractual Clauses**" or "**EU SCCs**");

1.1.8 "**Sub-processor**" means any third party (including any Mirion Affiliates) engaged by Mirion to process any Customer Personal Data (but shall not include Mirion employees or consultants);

1.1.9 "**Third Country**" means (i) where the EU GDPR or the FADP applies, a country outside of the European Economic Area, which is not subject to an adequacy decision by the European Commission; and (ii) where the UK GDPR applies, any country other than the UK, which is not subject to an adequacy finding by the Information Commissioner's Office ("**ICO**");

1.1.10 **"UK Addendum"** means the International Data Transfer Addendum to the EU Standard Contractual Clauses issued by the Information Commissioner's Office

under s.119A(1) of the Data Protection Act 2018, as such Addendum may be revised under Section 18 therein.

2 Data Processing

2.1 For the purposes of the Data Protection Legislation, Mirion is a Processor or Sub-Processor acting on behalf of the Customer, who is the Controller or Processor of the Personal Data. Where Customer processes the Data as a Processor on behalf of its own customers and Mirion acts as a Sub-Processor, Customer warrants that the instructions given to Mirion will be in accordance with the instructions to Customer by its own customers.

2.2 The nature, purpose and duration of the Processing, the categories of Personal Data and the categories of Data Subjects whose Personal Data is being Processed in connection with the Services are set out in Schedule 1 of this Agreement. Each Party shall comply with its obligations under applicable Data Protection Legislation in respect of any Personal Data it processes under the Agreement.

2.3 Customer will serve as the sole point of contact for Mirion with regard to any third party controllers of the Customer Personal Data. Mirion need not interact directly with (including seek any authorizations directly from) any such third party controllers (other than through regular provision of the Services to the extent required by the Services Agreement). Where Mirion would (including for the purposes of the EU SCCs) otherwise be required to provide information, assistance, cooperation, or anything else to such third party controllers, Mirion may provide it solely to Customer. Notwithstanding the foregoing, Mirion is entitled to follow the instructions of such third party with respect to such third party's Customer Personal Data instead of Customer's instructions if Mirion reasonably believes this is legally required under the circumstances.

2.4 Customer is solely responsible for the accuracy, quality, and legality of Customer Personal Data and the means by which Customer acquired Customer Personal Data. Customer represents and warrants that:

2.4.1 it has provided, and will continue to provide, all notice and obtained, and will continue to obtain, all consents, permissions and rights necessary under Data Protection Legislation for Mirion to lawfully process Customer Personal Data on Customer's behalf and in accordance with its instructions;

2.4.2 it has complied with all applicable Data Protection Legislation in the collection and provision to Mirion and its Sub-processors of such Customer Personal Data; and

2.4.3 it shall ensure its processing instructions comply with applicable laws (including Data Protection Legislation) and that the processing of Customer Personal Data by Mirion in accordance with the Customer's instructions will not cause Mirion to be in breach of applicable Data Protection Legislation.

2.5 Mirion shall comply with its obligations under the Data Protection Legislation and shall, in particular:

2.5.1 process the Personal Data only to the extent necessary for the purpose of providing the Services and in accordance with the Customer's written instructions (including with respect to transfers of Personal Data to a Third Country or to an International Organisation);

2.5.2 implement appropriate technical and organisational measures in accordance with the Data Protection Legislation to ensure a level of security appropriate to the risks that are presented by such Processing, in particular, from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data, taking into account the state of the art, the costs of implementation, the nature, scope, context and purposes of Processing and the likelihood and severity of risk in relation to the rights and freedoms of the Data Subjects as set out in Schedule 2;

2.5.3 ensure that any employees or other persons authorised to Process the Personal Data are subject to appropriate obligations of confidentiality;

2.5.4 on request by the Customer and taking into account the nature of the Processing and the information available to Mirion, assist the Customer in ensuring compliance with its obligations under the Data Protection Legislation in respect of the Personal Data;

2.5.5 engage any third party sub-processor to carry out its Processing obligations under this Agreement by way of a written contract that such third party will, at all times during the engagement, be subject to data processing obligations equivalent to those set out in this Agreement;

2.5.6 notify the Customer, as soon as reasonably practicable, about any request or complaint received from a Data Subject (without responding to that request, unless authorised to do so by the Customer) and assist the Customer by technical and organisational measures, insofar as possible, for the fulfilment of the Customer's obligations in respect of such requests and complaints;

2.5.7 notify the Customer on becoming aware of a Personal Data breach;

2.5.8 notify the Customer, unless prohibited from doing so under Data Protection Legislation, if it becomes aware that any data processing instruction from the Customer violates Data Protection Legislation or it is unable to comply with the Customer's data processing instructions, in which case, the Customer is entitled to withdraw or modify their processing instructions.

2.5.9 on request by the Customer, make available information necessary to demonstrate the Customer's compliance obligations under the Data Protection Legislation and on reasonable advance notice in writing permit, and contribute to, audits of compliance with Data Protection Legislation and this Agreement carried out by the Customer (or its authorised representative);

2.5.10 on termination or expiry of this Agreement, destroy, delete or return (as the Customer directs) all Personal Data and delete all existing copies of such data unless required by law to keep or store such Personal Data.

2.6 The Customer consents to the engagement sub-processors. This authorization will constitute Customer's prior written consent to the subcontracting by Mirion of the processing of Personal Data as required under the standard contractual clauses or the Data Protection Legislation.

2.7 Mirion may, from time to time, engage new sub-processors. Mirion will give Customer notice of any new sub-processor at least 30 days in advance of providing that sub-processor with access to Customer Data by updating the website and providing the Customer with a mechanism to obtain notice of that update. The Customer may object to Mirion's use of a new sub-processor by notifying Mirion promptly in writing within ten 10 business days after receipt of Mirion's notice in accordance with the mechanism set out in this Section 2.7. If the Customer does not approve of a new sub-processor, then the Customer may terminate the applicable Agreement(s) without liability with respect only to those Services that cannot be

provided by Mirion without the use of the objected-to new sub-processor by providing, before the end of the relevant notice period, written notice of termination.

2.8 The Customer acknowledges that clause 2.5.1 shall not apply to the extent that Mirion is required by law to Process the Personal Data other than in accordance with the Customer's instructions and Mirion acknowledges that, in such a case, it must promptly inform the Customer of the relevant legal requirement prior to Processing unless the law prohibits the provision of such information.

2.9 The Customer is responsible for reviewing the information made available by Mirion relating to data security and making an independent determination as to whether the Services meet Customer's requirements and legal obligations under the applicable Data Protection Legislation. Customer acknowledges that the Security Measures are subject to technical progress and development and that Mirion may update or modify the Security Measures from time to time provided that such updates and modifications do not result in a material degradation of the overall security of the Services subscribed to by the Customer.

2.10 If Mirion becomes aware that any law enforcement, regulatory, judicial or governmental authority outside the EEA, the UK and Switzerland (an "**Authority**") wishes to obtain access to or a copy of some or all Personal Data, whether on a voluntary or a mandatory basis, then unless legally prohibited as part of a mandatory legal compulsion that requires disclosure of Personal Data to such Authority, Mirion shall:

2.10.1 immediately notify Customer of such Authority's data access request;

2.10.2 inform the Authority that it is a Processor of Personal Data and that Customer has not authorised them to disclose that Personal Data to the Authority;

2.10.3 inform the Authority that any and all requests or demands for access to Personal Data should be notified to or served upon Customer in writing; and

2.10.4 not provide the Authority with access to Personal Data unless and until authorised by Customer.

2.11 In the event Mirion is under a legal prohibition or a mandatory legal compulsion that prevents them from complying with clause 2.10 in full, Mirion shall use reasonable and lawful efforts to challenge such prohibition or compulsion (Customer acknowledges that such challenge may

not always be reasonable or possible in light of the nature, scope, context and purposes of the intended Authority access request).

2.12 If Mirion makes a disclosure of Personal Data to an Authority (whether with Customer's authorisation or due to a mandatory legal compulsion) Mirion shall only disclose such Personal Data to the extent Mirion is legally required to do so and in accordance with applicable lawful process.

2.13 Clauses 2.10 to 2.12 shall not apply in the event that, taking into account the nature, scope, context and purposes of the intended Authority's access to the Personal Data, Mirion has a reasonable and good-faith belief that urgent access is necessary to prevent an imminent risk of serious harm to any individual. In such event, Mirion shall notify Customer as soon as possible following such Authority's access and provide Customer with full details of the same, unless and to the extent Mirion is legally prohibited from doing so.

2.14 Mirion shall not knowingly disclose Personal Data in a massive, disproportionate and indiscriminate manner that goes beyond what is necessary in a democratic society.

2.15 Mirion shall have in place and maintain in accordance with good industry practice measures to protect Personal Data from interception (including in transit from Customer to Mirion and between different systems and services). This includes having in place and maintaining network protection to deny attackers the ability to intercept data and encryption of Personal Data whilst in transit to deny attackers the ability to read data.

3 Data Transfers

3.1 Personal data that Mirion processes under the Agreement may be processed in any country in which Mirion, its Affiliates and authorized Sub-processors maintain facilities to perform the Services. Mirion shall not process or transfer Customer Personal Data (nor permit such data to be processed or transferred) outside of the EEA, Switzerland or the UK, unless it first takes such measures as are necessary to ensure the transfer is in compliance with this Agreement and applicable Data Protection Legislation.

3.2 The Parties agree that when the transfer of personal data from Customer (as "data exporter") to Mirion (as "data importer") is a Restricted Transfer and Data Protection Legislation requires that appropriate safeguards are put in place, such transfer shall be subject to the Standard Contractual Clauses, which shall be deemed incorporated into and form a part of this DPA as

set out in Schedule 3. It is not the intention of either party to contradict or restrict any of the provisions set forth in the Standard Contractual Clauses and, accordingly, if and to the extent the Standard Contractual Clauses conflict with any provision of the Services Agreement or this Agreement the Standard Contractual Clauses shall prevail to the extent of such conflict.

3.3 If Mirion adopts an alternative data export mechanism (including any new version of or successor to the Standard Contractual Clauses or Privacy Shield adopted pursuant to applicable Data Protection Legislation) for the transfer of personal data not described in this Agreement ("**Alternative Transfer Mechanism**"), the Alternative Transfer Mechanism shall apply instead of any applicable transfer mechanism described in this Agreement (but only to the extent such Alternative Transfer Mechanism complies with applicable Data Protection Legislation and extends to the territories to which the relevant personal data is transferred).

4 General

4.1 This Agreement shall be governed by the law of France.

Schedule 1

Data Processing

List of parties	
Controller or Processor / Data exporter	Customer
Processor or Sub-Processor / Data Importer	Mirion Technologies (Dosimetry Services), B.V., NL ***OR*** Mirion Technologies (AWST) GmbH, DE ***OR*** Mirion Technologies (GDS), Inc., US Contact person: Edwin Ulbricht email: privacy@mirion.com
Description of the processing / transfer	
Nature/purpose of Processing	The data importer provides dosimetry services e.g., services to measure and track exposure to ionizing radiation for occupational and other safety purposes. The provision of dosimetry services is the activity relevant to the transfer of personal data. The personal data being transferred pertains to the individual employees covered by the data exporter's radiation monitoring programs and for which data exporter procures dosimetry services from the data importer.
Categories of Data Subjects	Employees of the data exporter or data exporter's own customers covered by the data exporter's or data exporter's customers radiation monitoring programs and for which data exporter procures dosimetry services from the data importer.
Categories of Personal Data	• Full name • Gender • Identification numbers as required by applicable regulations • Date of birth • Occupation, employer • Occupational/Industry category • Start date and end date of monitoring • Email address • Home address

	In all cases the personal data are limited to what is technically necessary and/or legally required
Special Categories of Personal Data	Radiation dose. In addition, the personal data may – but does not necessarily - include the pregnancy start and end dates of the data subject.
Third Countries or International Organisations Personal Data will be transferred to	United States of America
Frequency of the Transfer (e.g. whether the data is transferred on a one-off or continuous basis):	Continuous
Duration of the Processing:	For the term of the underlying Services Agreement until deletion of the personal data by Mirion in accordance with the Services Agreement and/or applicable law.
Period for which the Personal Data will be retained, or if that is not possible the criteria used to determinate that period, if applicable:	Mirion will retain the Customer Personal Data for the duration of this Agreement and for any period after the termination or expiration of this Agreement in accordance with the terms set forth herein or with any applicable retention obligations.
Sub-Processors	Cloud-based hosting services are provided by: • Microsoft Corporation, USA

Schedule 2

Technical and Organizational Measures

Description of the technical and organizational security measures implemented by Mirion:

Mirion Technologies Cybersecurity and Data Protection Program
is available here: *https://www.mirion.com/legal/cybersecurity-and-data-protection-program*.

Technical and Organisation Measures implemented in addition in the context of dosimetry services:

1. BeOSL, TLD and Film Dosimeters

These are dosimeters that are physically sent to Mirion dosimetry services for read-out.

- Raw dose data stored on the dosimeters are encrypted as the dosimeters can only be read out by Mirion dosimetry services using proprietary tools and processes.
- Processing and storage of raw dose data and dose records occur on systems internal to Mirion and secured according to Mirion's Cybersecurity and Data Protection Program available here: https://www.mirion.com/legal/cybersecurity-and-data-protection-program.
- Data at rest are encrypted.
- Access to data by Mirion personnel is restricted to data required in order to perform assigned tasks.
- Access to dose records by customer personnel occurs through dedicated web services that in turn access the data on the internal servers. Access is strictly restricted to data within the customer account.
- Access to web services by customers is secured by TLS and is restricted to the information and functionality required by the role of the user. Passwords of user accounts have to meet complexity requirements and are stored as a SHA-256 hash in an encrypted database.
- To the extent that servers are hosted by authorized sub-processors, such sub-processors implement adequate technical and organizational measures that are documented in the applicable data processing agreement.

2. Instadose

These are dosimeters that remain at the customer facility and transmit dose information electronically to Mirion Technologies dosimetry services.

- All data in transit between a data transmission device/software and internal servers are encrypted using TLS 1.2 w/SHA-265.

- Raw dose data are intrinsically encrypted as they can only be transformed into human readable dose records by Mirion proprietary algorithms.
- Raw dose data are not stored on any device/software used to transmit data from the Instadose dosimeter to internal servers. Raw dose data are solely stored in the Instadose dosimeter and on internal servers.
- Devices/software used to transmit raw dose data are hardened by removing all unnecessary components. No remote access to these devices/software is required.
- Instadose data transmission devices authenticate the Instadose dosimeter prior to accepting the raw dose data for transmission.
- Internal servers verify the raw dose data's integrity before accepting it from the transmission device.
- Dose records generated from raw dose data are not accessible from, via or on the Instadose dosimeter.
- Internal servers are accessible only to Mirion personnel and are secured according to Mirion's Cybersecurity and Data Protection Program available here: https://www.mirion.com/legal/cybersecurity-and-data-protection-program.
- Data at rest are encrypted.
- Access to data by Mirion personnel is restricted to data required in order to perform assigned tasks.
- Access to dose records by customer personnel occurs through dedicated web services that in turn access the data on the internal servers. Access is strictly restricted to data within the customer account.
- Access to web services by customers is secured by TLS and is restricted to the information and functionality required by the role of the user. Passwords of user accounts have to meet complexity requirements and are stored as a SHA-256 hash in an encrypted database.
- To the extent that servers are hosted by authorized sub-processors, such sub-processors implement adequate technical and organizational measures that are documented in the applicable data processing agreement.

Schedule 3

Standard Contractual Clauses

(a) In relation to transfers of Customer Personal Data that is protected by the EU GDPR, the EU SCCs shall apply, completed as follows:

i. Module Two (Controller to Processor) or Module Three (Processor to Processor) will apply (as applicable);

ii. in Clause 7, the optional docking clause will apply;

iii. in Clause 9, Option 2 will apply, and the time period for prior notice of Sub-processor changes shall be as set out in Section 2.5 of this Agreement;

iv. in Clause 11, the optional language will not apply;

v. the competent supervisory authority shall be the supervisory authority defined in accordance with Clause 13(a);

vi. in Clause 17, Option 1 will apply, and the EU SCCs will be governed by the law of France;

vii. in Clause 18(b), disputes shall be resolved before the courts of France

viii. Annex I of the EU SCCs shall be deemed completed with the information set out in Schedule 1 to this Agreement; and

ix. Subject to Section 5.2 of this Agreement, Annex II of the EU SCCs shall be deemed completed with the information set out in Schedule 2 to this Agreement;

(b) In relation to transfers of Customer Personal Data protected by the FADP, the EU SCCs will also apply in accordance with paragraph (a) above, with the following modifications:

i. references to "Regulation (EU) 2016/679" shall be interpreted as references to FADP;

ii. references to specific Articles of "Regulation (EU) 2016/679" shall be replaced with the equivalent article or section of the FADP;

iii. references to "EU", "Union", "Member State" and "Member State law" shall be replaced with references to "Switzerland" or "Swiss law" (as applicable);

iv. the term "member state" shall not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (i.e., Switzerland);

v. notwithstanding Clause 13(a) the "competent supervisory authority" is the Swiss Federal Data Protection Information Commissioner;

vi. references to the "competent supervisory authority" and "competent courts" shall be replaced with references to the "Swiss Federal Data Protection Information Commissioner" and "applicable courts of Switzerland";

vii. in Clause 17, the Standard Contractual Clauses shall be governed by the laws of Switzerland; and

viii. Clause 18(b) shall state that disputes shall be resolved before the applicable courts of Switzerland.

(c) In relation to transfers of personal data protected by UK GDPR, the EU SCCs shall: (i) apply as completed in accordance with paragraph (a) above; and (ii) be deemed amended as specified by Part 2 of the UK Addendum, which shall be deemed incorporated into and form an integral part of this Agreement. In addition, tables 1 to 3 in Part 1 of the UK Addendum shall be completed respectively with the information set out in Schedule 1 and 2 of this Agreement and table 4 in Part 1 shall be deemed completed by selecting "neither party".