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

BETWEEN

(1) **Sun Nuclear B.V.** incorporated and registered in [Netherlands] with company number 78485169 whose registered office is at Verlengde Poolseweg 36, 4818CL Breda with mailing address Verlengde Poolseweg 36, 4818CL Breda, Netherlands;

Sun Nuclear GmbH incorporated and registered in Germany with District Court Kiel under HRB 23271 KI whose registered office is at Gutenbergring 67 A, 22848 Norderstedt with mailing address Gutenbergring 67 A, 22848 Norderstedt, Germany;

(hereinafter individually and collectively referred to as "**Sun Nuclear**")

and

(2) The legal entity that is party to and executed the underlying Services Agreement as a Customer;

(hereinafter individually referred to as "**Customer**").

BACKGROUND

(A) Sun Nuclear provides, consultancy and repair and maintenance services ("**Services**") to the Customer pursuant to an agreement ("**Services Agreement**") underlying this Agreement.

(B) This Agreement forms part of and is incorporated by reference into the Services Agreement entered into by the Customer and Sun Nuclear concerning Customer's use of the Services to reflect the parties' agreement regarding the Processing of Personal Data in accordance with the applicable 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) The Sun Nuclear entity that is party to the Services Agreement is party to this DPA.

(D) This Agreement consists of the terms described herein, Schedule 1 and Schedule 2 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 "**Data Protection Legislation**" shall mean one or more of the following as may be applicable to the Personal Data Processed by Sun Nuclear 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.

1.1.2 "**Standard Contractual Clauses**" means: (i) 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**"); and (ii) where the UK GDPR applies, (a) for so long as it is lawfully permitted the standard contractual clauses for the transfer of personal data to processors set out in the European Commission's Decision 2010/87/EU of 5 February 2010 adopted pursuant to or permitted under Article 46 of the UK GDPR ("**Prior UK SCCs**"); and (b) where sub-clause 1.1.2 (ii)(a) does not apply, and the respective parties are lawfully permitted to rely on the EU SCCs for transfers of personal data from the United Kingdom subject to

completion of a “UK Addendum to the EU Standard Contractual Clauses” (“**UK Addendum**”) issued by the Information Commissioner’s Office under s.119A(1) of the Data Protection Act 2018, the EU SCCs, subject to the execution of the UK Addendum amended as specified by the UK Addendum;

1.1.3 “**Data Subject**”, “**Controller**”, “**International Organisation**”, “**Personal Data**”, “**Processor**” and “**Processing**” have the same meaning as in the applicable Data Protection Legislation;

1.1.4 "**Third Country**" means : (i) where the EU GDPR applies, a country outside of the European Economic Area which is not subject to an adequacy decision by the European Commission; (ii) where the FADP applies, a country outside of the European Economic Area which is not subject to an adequacy decision by the European Commission; and (iii) 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**").

2 Data Processing

2.1 For the purposes of the applicable Data Protection Legislation, Sun Nuclear is a Processor acting on behalf of the Customer, who is the Controller of the Personal Data.

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.

2.3 Sun Nuclear shall comply with its obligations under the applicable Data Protection Legislation and shall, in particular:

2.3.1 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);

2.3.2 implement appropriate technical and organisational measures, set out in Schedule 2 to this Agreement in accordance with the applicable 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;

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

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

2.3.5 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 and

2.3.6 where the sub-processor is located in a Third Country have ensured appropriate safeguards and procured the entering into of the Standard Contractual Clauses (or such other agreement which may be approved from time to time as providing an adequate level of protection for Personal Data);

2.3.7 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;

2.3.8 notify the Customer immediately and not later than 24 hours on becoming aware of a Personal Data breach;

2.3.9 on request by the Customer, make available information necessary to demonstrate the Customer's compliance obligations under the applicable Data Protection Legislation and on reasonable advance notice in writing

permit, and contribute to, audits of compliance with applicable Data Protection Legislation and this Agreement carried out by the Customer (or its authorised representative);

2.3.10 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.

2.4 The Customer consents to the engagement sub-processors. This authorization will constitute Customer's prior written consent to the subcontracting by Sun Nuclear of the processing of Personal Data as required under the applicable Standard Contractual Clauses or the applicable Data Protection Legislation.

2.5 Sun Nuclear may, from time to time, engage new sub-processors. Sun Nuclear will give Customer notice of any new sub-processor at least 1 months in advance of providing that sub-processor with access to Customer Data. The Customer may object to Sun Nuclear's use of a new sub-processor by notifying Sun Nuclear promptly in writing within ten 10 business days after receipt of Sun Nuclear's notice in accordance with the mechanism set out in this Section 2.5. 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 Sun Nuclear without the use of the objected-to new sub-processor by providing, before the end of the relevant notice period, written notice of termination.

2.6 The Customer acknowledges that clause 2.3.1 shall not apply to the extent that Sun Nuclear is required by law to Process the Personal Data other than in accordance with the Customer's instructions and Sun Nuclear 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.

2.7 If Sun Nuclear 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, Sun Nuclear shall:

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

2.7.2 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;

2.7.3 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

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

2.8 In the event Sun Nuclear is under a legal prohibition or a mandatory legal compulsion that prevents them from complying with clause 2.7 in full, Sun Nuclear 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).

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

2.10 Clauses 2.7 to 2.9 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, Sun Nuclear 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, Sun Nuclear 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 Sun Nuclear is legally prohibited from doing so.

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

2.12 Sun Nuclear 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 Sun Nuclear 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 General

3.1 This Agreement shall be governed by the law of the Netherlands.

Schedule 1

Data Processing

List of parties	
Controller / Data Exporter	The Party identified as the Controller in the Agreement
Processor / Data Importer	The Sun Nuclear entity identified as the Processor in the Agreement Contact person and DPO: Fernando Otero 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 are the activities 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.
Duration of Processing	For the duration of the Services Agreement.
Categories of Data Subjects	Patients and employees of the Customer.
Categories of Personal Data	Full name. Date of birth of patients. Email addresses of employees.
Special Categories of Personal Data	Gender of patients. Personal data concerning health limited to the medical record number.
Third Countries or International Organisations Personal Data will be transferred to	United States of America
Sub-Processors	Sun Nuclear Corp., Melbourne FL, USA

Schedule 2

Description of the technical and organisational security measures implemented by Sun Nuclear:

Mirion Technologies Cybersecurity and Data Protection Program as of 13 September 2021

Controls Category	Mirion Practice
Governance (ID.GV)	Governance Framework: Mirion's Cybersecurity and Data Protection program is based on the National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF 1.1) and Special Publication (SP) 800:53 Rev 5. Policies: Mirion periodically reviews and updates the Cybersecurity Policies and Standards in accordance with industry standards. Assurance: Mirion has established periodic, independent assessments to ensure that Cybersecurity Policies, Standards, and Controls are implemented in accordance with internal policy and standards.
Asset Management (ID.AM)	Asset Management: Mirion maintains an inventory of system and software assets and related configuration metadata. Asset Classification: Mirion's information assets are assigned a classification level based on its level of sensitivity and the impact to the organization in order to appropriately restrict access and ensure the appropriate minimum baseline standards (low, medium, high) are implemented in accordance with NIST 800.53 Rev 5.
Risk Assessment (ID.RA)	Vulnerability Management: Mirion utilizes scanning tools to assess systems, services, and applications on a periodic basis in accordance with internal policies. • • Identified vulnerabilities are risk assessed, resolved and/or mitigated in a timely manner in accordance with internal policies. • • Ad-hoc scans are performed as necessary when new vulnerabilities are identified that affect Mirion systems, services, and applications • • Scanning tools are updated to the latest vulnerability databases on a routine basis in accordance with internal policies Threat Hunting: Mirion has established a dedicated security team to proactively search for Indicators of Compromise (IoC) and to detect, track and disrupt threats that evade existing security controls in Mirion systems, applications, and services.
Risk Management Strategy (ID.RM)	Governance Structure: Mirion has a dedicated group, Digital Security Services (DSS), reporting to the Chief Information Security Officer (CISO), that centrally operates the Cybersecurity and Data Protection Program at an enterprise level to address Mirion's applicable statutory, regulatory, and contractual obligations. Additionally, a dedicated team within the DSS organization manages Cyber Risk, Governance, and Compliance. Risk Assessment: Mirion's CISO organization conducts periodic risk assessments and communicates to executive leadership.
Supply Chain Risk Management (ID.SC)	Review of General IT and Security Controls: Mirion identifies and verifies General IT Controls and Security controls on a recurring basis in accordance with internal policies. This may include reviews based on inquiry, independent audit reports (e.g., SOC 1), or other IT certification documents based on the vendor risk and in accordance with internal policies.
Identity Management, Authentication and Access Control (PR.AC)	Identity and Authentication Policy: Mirion requires proper user identification and authentication management for all standard and privileged users on all systems, applications, and services • • Unique user IDs are required • • Shared, group, generic, and anonymous end user accounts are specifically prohibited, unless specifically approved by the Office of the CISO. • • Authentication mechanisms are based on data classification and system impact. • • At a minimum, multi-factor authentication is required for access to Mirion network

	• • Minimum password standards are enforced in accordance with industry standards and internal policy, which include, at a minimum: password length, password complexity, password expiration, password lockout, and password re-use. Access Control Policy: Mirion limits access to its systems and data to authorized users. • • Documentation of the addition, deletion and modification of user IDs, credentials and other identifier objects is maintained to verify authorized access to Mirion systems and data • • User access is revoked timely and in accordance with internal policy to all Mirion systems and data • • Appropriate segregation of duties is maintained Least Privilege: Mirion restricts access to systems and data to only those individuals who require such access to perform their job function. Privileged User Accounts: Privileged user accounts are assigned in accordance with job classification and function and based on a least-privileged approach and "deny all" unless specifically allowed. Physical Access: Mirion restricts and monitors access to facilities where information systems are located.
Awareness and Training (PR.AT)	Security Training. Mirion requires Security Awareness Training for its employees in accordance with internal policy. Acceptable Use: Mirion has an established Acceptable Use Policy that governs the acceptable and unacceptable use of computing and communications for accounts, devices, and network resources.
Data Security (PR.DS)	Data Backup: Mirion backups systems and data on a regular basis in accordance with internal policies. Access to backups is appropriately restricted to authorized personnel. Data Classification: Mirion assigns a sensitivity level for data based on the appropriate audience and impact of the system. Regulatory, legal, contractual, and/or company directives supersede standard classification levels. The standard data sensitivities are as follows: restricted, confidential, internal use, and public. Data Discovery: Mirion performs periodic data discovery and data classification reviews in accordance with internal policies and regulatory statutes. Data Encryption: Mirion encrypts data at-rest and in-transit in accordance with internal policies and data classification.
Information Protection Processes and Procedures (PR.IP)	Secure System Development Life Cycle: Mirion products and solutions apply product security design guidelines during engineering process in accordance with internal policies. The security standards are designed based on industry best practices and governed by Mirion CISO organization. Product security standards addresses the need of hardware, firmware, operating system, application, data, and network security as appropriate and applicable to product/solution. System Environments: Mirion maintains separate development, testing, and production environments. Pre-Employment Screening: Appropriate background checks are completed for employees and contractors in prior to employment in accordance with internal policy. Confidentiality Agreements: Mirion ensures employees and contractors sign confidentiality agreements in accordance with internal policy. Security Policy Compliance: Any person subject to Mirion's Cybersecurity Policies and Standards, who fails to comply with the provisions are subject to appropriate disciplinary or legal action in accordance with the Mirion's Disciplinary Code and Procedures.
Threat Intelligence and Incident Management *	Penetration Testing: Mirion performs periodic penetration testing on systems, applications, and services in accordance with internal policies. Event Logging: Mirion enables system logging, where technologically feasible, of defined events in accordance with internal policies. The logs are centrally managed and monitored on a periodic basis, where potential security issues are investigated and resolved. Malicious Code: Mirion Technologies uses security software and technology to protect against malicious code. Security Incident Response Policy: Mirion has a dedicated security team to assess, mitigate, investigate, document, and report security incidents in accordance with internal policy.

	• • Mirion ensures appropriate incident data collection and notifications in accordance with applicable laws, standards, and internal policy. Data Retention: Mirion retains data in accordance with applicable statutory, regulatory, and contractual obligations. Access to off-site storage media is appropriately restricted to authorized individuals. Data Recovery: Mirion periodically performs data recovery procedures in accordance with internal policies to ensure data is available and recoverable.

*Includes NIST Security Control Categories: Protective Technology, Anomalies and Events, Security Continuous Monitoring, Detection Processes, Response Planning, and Recovery Planning