Sistema Socio Sanitario

Ospedale Papa Giovanni XXIII

Regione Lombardia

ASST Papa Giovanni XXIII

DELIBERAZIONE NR. 1474 DEL 04/09/2025

OGGETTO: AUTORIZZAZIONE ALL'AVVIO DELLO STUDIO RECLAIMS (REG. 0179-2024) PRESSO LA SC NEUROLOGIA DI CUI È PROMOTORE CHARITÈ – UNIVERSITÄTSMEDIZIN BERLIN.

IL DIRETTORE GENERALE
nella persona del dott. Francesco Locati

ASSISTITO DA:

IL DIRETTORE AMMINISTRATIVO	DR. GIANLUCA VECCHI
IL DIRETTORE SANITARIO AD INTERIM	DOTT. FRANCESCO LOCATI
IL DIRETTORE SOCIO SANITARIO	DR.SSA SIMONETTA CESA

Premesso che:

- con deliberazione nr. 622 del 10/04/2025 è stato autorizzato l'avvio del progetto di ricerca "CLAIMS" - Grant Agreement n. 101112153 - approvato e finanziato dalla Commissione europea nell'ambito del programma di finanziamento Horizon Europe;
- come previsto dal progetto stesso, il capofila Charitè – Universitätsmedizin Berlin ha proposto la conduzione presso la SC Neurologia di questa azienda, in qualità di centro partecipante, dello studio RECLAIMS (reg. 0179-2024), con titolo: "Clinical Impact through AI-assisted MS care: a retrospective multi-center observational study";

Richiamato il "Regolamento aziendale per la gestione delle sperimentazioni e collaborazioni scientifiche. rev. 1.0" approvato con deliberazione n. 2110 del 29/12/2015;

Rilevato che il dott. Dario Alimonti, direttore f.f. della SC Neurologia, ha manifestato la disponibilità alla gestione dello studio per gli aspetti scientifici e clinici, presso la propria struttura, proponendosi quale sperimentatore principale;

Atteso che il direttore f.f. della SC ha fornito alla SC Ricerca clinica, sviluppo e innovazione la documentazione e i dati necessari per la valutazione delle caratteristiche dello studio e per la definizione della fattibilità locale;

Precisato che:

- trattasi di studio no-profit, con validità fino al 31/12/2025 senza la ripartizione di alcun compenso tra quanti collaborano allo stesso;

- l’analisi di fattibilità locale ha dato esito positivo, come risulta dalla documentazione agli atti;
- in conformità con l'art. 9 del GDPR e con l'art. 110, come modificato, del “Codice privacy” (d.lgs. n. 196/2003 e d.lgs. n. 101/2018), i dati personali saranno utilizzati a scopi di ricerca scientifica senza il previo consenso esplicito degli interessati, qualora non sia possibile acquisirlo;
- la valutazione d’impatto relativa al trattamento dati personali (DPIA) dello studio ha dato esito positivo, come risulta dalla documentazione agli atti;

Vista la proposta di convenzione Data Processing Agreement (DPA) relativa allo studio in esame, ritenuta idonea a disciplinare gli impegni delle parti;

Preso atto che il Comitato etico territoriale Lombardia 6 ha espresso parere favorevole in data 25/03/2025;

Dato atto che la dr.ssa Monia Maria Beatrice Lorini, direttore della SC Ricerca clinica, sviluppo e innovazione, è responsabile del procedimento;

Acquisito il parere del direttore amministrativo, del direttore sanitario ad interim e del direttore sociosanitario

DELIBERA

1. di autorizzare l’avvio dello studio RECLAIMS (reg. 0179-2024), con titolo: “Clinical Impact through AI-assisted MS care: a retrospective multi-center observational study” proposto dal promotore Charitè – Universitätsmedizin Berlin, presso la SC Neurologia;
2. di affidare la responsabilità di sperimentatore principale al dott. Dario Alimonti;
3. di sottoscrivere, con i partner del progetto CLAIMS che partecipano allo studio, la DPA relativa allo studio citato, nel testo allegato al presente atto, al quale si fa espresso rinvio (all. A);
4. di dare atto che la dr.ssa Monia Maria Beatrice Lorini, direttore della SC Ricerca clinica, sviluppo e innovazione, è responsabile del procedimento.

IL DIRETTORE GENERALE
Dott. Francesco Locati

Data Processing Agreement

CLAIMS – RECLAIM study

26/08/2025

Version 2.0

This project is supported by the Innovative Health Initiative Joint Undertaking (JU) under grant agreement No 101112153. The JU receives support from the European Union's Horizon Europe research and innovation programme and COCIR, EFPIA, EuropaBio, MedTech Europe, Vaccines Europe, AB Science SA and icometrix NV.

Data Processing Agreement

Between:

- **General University Hospital Prague (GUHP),** established by the decision of the Ministry of Health of the Czech Republic dated 25 November 1990
- **Charité – Universitätsmedizin Berlin (CHARITE),** established in Charitéplatz 1, Berlin 10117 Germany
- **Technische Universität Dresden (TUD),** established in 01062 Dresden, represented by the Chancellor; Acting side: Carl Gustav Carus Faculty of Medicine, Fetscherstraße 74, 01307 Dresden
- **Ruhr-Universität Bochum (RUB),** established in Universitätsstraße 150, 44801 Bochum, Germany
- **Azienda Socio Sanitaria Territoriale Papa Giovanni XXIII (PG23),** established in Piazza OMS - Organizzazione Mondiale della Sanità 1, 24127 Bergamo, Italy
- **F. Hoffmann-La Roche (ROCHE),** established on October 1, 1896, at the age of 28, Fritz Hoffmann-La Roche launched his company as the successor company to Hoffmann, Traub & Co in Basel, Switzerland
- **Bristol Myers Squibb (BMS),** established in in 1989, Co 0020 ER Squibb & Sons LLC (USA)
- **AB Science (ABSCIENCE),** established in 3 avenue George V, 75 008 Paris, France

Hereafter referred to as the "Supplying Data Controllers".

And:

- **ICOMETRIX NV (ICOMETRIX)**, established in KOLONEL BEGAULTLAAN 1B, LEUVEN 3012, Belgium, VAT number: BE0833377379
- **AALTO University Foundation sr. (AALTO),** established in P.O. Box 11000, 00076 AALTO Finland, VAT-code: FI22283574
- **Nocturne GmbH (NOC),** established in Schönhauser Allee 177, 10119 Berlin, Germany
- **Neuroquantic srl (NEUROQUANTIC)**, established in Via Papa Giovanni XXIII n. 21, 20093 Cologno Monzese (Milan, Italy)

Hereafter referred to as the "Receiving Data Controllers".

Collectively referred to as "Parties" or "Party".

All parties to this Agreement are collectively referred to as the 'Parties' or a 'Party'.

Table of Contents

DEFINITIONS

"**Anonymous**", "**Anonymisation**" or "**Anonymised**" means that the concerned data no longer relate to an identified or identifiable natural person. This means that Personal Data are rendered Anonymous in such a manner that the Data Subject is not or no longer identifiable (e.g., because all direct and indirect personal identifiers are removed from the data by for instance implementing technical measures so that such data can no longer be linked back to the initial Data Subject and the Data Subject can therefore not be re-identified).

"**Confidential Information**" means any data, documents or other material (in any form) that is identified as confidential at the time it is disclosed. If information has been identified as confidential only orally, it will be considered to be Confidential Information only if such confidentiality is confirmed in writing within thirty (30) Days of the oral disclosure. Notwithstanding the foregoing, personal data will always be considered as Confidential Information.

"**Consortium**" means the group of Beneficiaries that are parties to the CLAIMS Consortium Agreement.

Receiving Data Controllers - The Receiving Data Controllers are the Parties that do not contribute any data to the Project but instead process personal data obtained from the Supplying Data Controllers.

Supplying Data Controllers - The Supplying Data Controllers are the Parties that initially gathered the personal data and are now making this data available within the context of the Project. They might also participate in the processing of the data.

"**Processor**" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

PRELIMINARY PROVISIONS

This Agreement covers the processing activities entrusted to the Parties within the framework of "the CLAIMS project ("Clinical Impact through AI-Assisted MS Care") funded by the European Union's Horizon Europe programme under EU Grant number: 101112153" (hereafter referred to as the "Project").

The intention of this Data Processing agreement (the "Agreement") is to regulate the processing activities performed by the Receiving Data Controllers and Processor(s) with the data of the Supplying Data Controllers pursuant to the Regulation 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 (hereafter referred to as 'GDPR', General Data Protection Regulation) and to the extent applicable, the Data Protection Act 2018, and the Privacy and Electronic Communications (EC Directive) Regulations 2003, all as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) EU Exit Regulations 2019.

The terms 'controller', 'data subject', 'processor', 'personal data', 'personal data breach', 'processed', 'processing' and 'pseudonymisation' shall have the meaning given to those terms in the GDPR.

The Agreement shall ensure that personal data relating to the data subjects is not used unlawfully or comes into the hands of a third party.

The Agreement stipulates the rights and obligations of the Supplying Data Controllers and the Receiving Data Controllers.

COPYRIGHT AND DISCLAIMER

ARTICLE 1 : SUBJECT MATTER OF THE AGREEMENT

The details concerning the processing activities performed by the Receiving Data Controllers with the personal data of the Supplying Data Controllers are specified in **Appendix 1**, which forms an integral part of this Agreement.

Only personal data which is mentioned in **Appendix 1** may and shall be processed by the Receiving Data Controllers. Furthermore, personal data shall only be processed by the Receiving Data Controllers considering the purpose(s) and processing activities which are specified in **Appendix 1**.

The Supplying Data Controllers shall ensure that the personal data are at least pseudonymised before transfer to the Receiving Data Controllers; and that only the variables and personal data that is needed to perform the processing by that Receiving Data Controller (**Appendix 1**) are transferred.

Supplying Data Controllers may at times also receive, and process personal data from other Supplying Data Controllers and shall then be considered as Receiving Data Controllers under this Agreement.

When processing personal data for the purpose of the Project, Supplying and Receiving Data Controllers shall do so in accordance with this Agreement.

A Processor shall only process the Personal Data on documented instructions from the Controllers. The Processor may not process Personal Data for any purpose other than the purposes set out in this Agreement, or other than provided in the instructions, including in case of international Personal Data transfers, unless the Processor is required to do so by applicable laws to which the Processor is subject to. In such a case, the Processor shall inform the Controllers in writing of the legal requirement before processing, unless the law prohibits such information on important grounds of public interest.

Any subsequent instructions may also be given by the Controllers throughout the duration of the Processing of Personal Data, provided that such instructions are documented and kept in writing (including by email).

Any Processing carried out by the Processor for its own purposes without the Controller's authorisation shall be deemed to be carried out in breach of the Controller's instructions and Data Protection Laws.

ARTICLE 2 : DURATION OF THE PROCESSING

This Agreement shall be effective until one year after the end of the Project to allow finishing any ongoing research. This Agreement shall become effective and binding as to each Party individually upon such Party's execution of this Agreement, regardless of whether all other Parties have executed it at that time. The effectiveness of this Agreement with respect to any Party shall not be contingent upon execution by any other Party, and no Party shall be prevented from performing or exercising its rights under this Agreement solely due to the non-signature or delayed signature of another Party. Each Party agrees that its obligations and rights under this Agreement shall be fully enforceable as of the date it signs, with respect to all other Parties who have executed the Agreement at that time or subsequently.

At the end of this Agreement the Supplying Data Controllers declare to maintain a copy of their personal data for at least 10 years after the end date of this Agreement, to enable reproducibility of the results and to allow updating the software and results in line with the RECLAIM study protocol. The Receiving Data Controllers and Processor shall destroy their copy of the personal data after a period of maximum 2 years after the Project has ended.

Icometrix, as project leader and on behalf of the CLAIMS consortium, will retain a copy of the whole database for at least 15 years and/or upon regulatory or quality requirements and/or upon novel agreement between the partners, whichever is longer, after the end date of this Agreement, to enable

reproducibility of the results, to comply with regulatory requirements, and to allow updating the software and results in line with the RECLAIM study protocol.

ARTICLE 3 : APPLICABLE LEGISLATION

The Parties explicitly commit to comply with the requirements of the GDPR and any other applicable regulations to which the Parties are subject including but not limited to respective country-specific regulation with regard to the processing of personal data.

ARTICLE 4 : DATA SUPPLYING CONDITIONS

The Receiving Data Controllers process the personal data only in accordance with **Appendix 1 and 2** and shall not further process the personal data subject to this Agreement, in particular in a manner which is incompatible with the provisions laid down in this Agreement.

The Receiving Data Controllers shall immediately inform the Supplying Data Controllers if, in its opinion, this Agreement or actions of its Processor or Parties infringes the GDPR, or other Union or Member State's data protection provisions to which a Processor or Receiving Data Controller is subject.

ARTICLE 5 : THE USE OF (SUB-)PROCESSOR

The Receiving Data Controllers shall not engage a (Sub-)Processor other than for business-as-usual purposes (such purposes are not related to this Agreement and the Agreement's purposes as described in Appendix 1), without the prior consent of the Supplying Data Controllers. For the (Sub-)Processors engaged by the Receiving Data Controllers, listed in Appendix 1, this consent shall be given by means of signature of this Agreement.

In case a Receiving Data Controller engages a (Sub-)Processor for carrying out specific processing activities, the same personal data protection obligations as set out in this Agreement shall be imposed on that (Sub-)Processor by way of a contract, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of the GDPR.

Where a (Sub-)Processor fails to fulfil its personal data protection obligations, the Supplying or Receiving Data Controller responsible for that (Sub-)Processor shall remain fully liable for the performance of that Sub-Processor's obligations.

ARTICLE 6 : CONFIDENTIALITY

The Receiving Data Controllers and Processor commit to handling the personal data and its processing with highest confidentiality and in accordance with the terms and conditions of the Consortium Agreement for the Project entered into by the Parties.

Each Receiving Data Controller and Processor ensures that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

ARTICLE 7 : SECURITY MEASURES

The Supplying Data Controllers, together with the Receiving Data Controller, are jointly responsible for identifying and enabling a means of secure transfer of the personal data to the Receiving Data Controller.

Receiving Data Controllers and Supplying Data Controllers shall implement all appropriate technical and organizational measures in such a manner that processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subject.

Receiving Data Controllers and Supplying Data Controllers shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, according to Article 32 of the GDPR.

In assessing the appropriate level of security, particular account was taken of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data that is transmitted, stored or otherwise processed.

A general description of the technical and organizational security measures is included in **Appendix 2** to this Agreement.

ARTICLE 8 : RIGHTS OF DATA SUBJECTS

The Data Controllers shall assist each other by appropriate technical and organizational measures for the fulfilment of their obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR: right to be informed, right of access, rectification, erasure and objection, right to limitation of processing, right to portability of data, right not to be subject to automated individual decision making (including profiling). Where the persons concerned make requests to one of the Parties to exercise their rights, the latter must inform, without undue delay and no later than within two weeks, the Data Protection Officers of the Parties concerned.

The communication between the Parties of the information referred to in Articles 13 and 14 of the GDPR shall be free of charge, unless the requests of a data subject are unfounded or excessive.

ARTICLE 9 : REGISTER OF CATEGORIES OF PROCESSING ACTIVITIES

Supplying and Receiving Data Controllers and their representatives undertake to keep records of all categories of processing activities carried out, in accordance with Article 30.1 of the GDPR.

ARTICLE 10 : ASSISTANCE BETWEEN PARTIES

The Data Controllers shall assist each other in ensuring compliance with their obligations pursuant to the GDPR.

In the case of a personal data breach related to the processing subject of this Agreement, the Data Controllers shall notify each other within 24 hours after becoming aware of a personal data breach. Each of the Controllers involved shall individually do an assessment of whether or not this needs to be reported to the supervisory authority and/or the data subjects, and inform the other Parties involved of their decision.

This notification shall at least include following information:

- the nature of the personal data breach;
- the categories of personal data;
- the categories and approximate number of data subjects concerned;
- the categories and approximate number of personal data records concerned;
- the measures that have been taken to remedy the Personal Data breach, including, where appropriate, measures to limit the adverse effects and possible risks;

- the circumstances of the data leakage and a summary of the incident that led to the Personal Data breach;
- the presumed date of the incident;
- the likely consequences of the data leakage for the Data Subjects;
- the contact details of a contact point from which further information can be obtained.

The Data Controllers shall assist each other as they carry out a data protection impact assessment (DPIA) in accordance with Article 35 of the GDPR.

ARTICLE 11 : TRANSFER TO THIRD PARTIES

Any party not a party to this Agreement is considered a third party.

The transfer to third parties, in any manner possible is prohibited unless it's legally required or in case a Receiving Data Controller has obtained the explicit written consent by the Supplying Data Controllers to do so. In case a legal obligation to transfer personal data, which are subject to this Agreement, to third parties, applies, a Receiving Data Controller shall – prior to the transfer – notify the concerned Supplying Data Controllers.

ARTICLE 12 : TRANSFER TO THIRD COUNTRIES OR AN INTERNATIONAL ORGANIZATION

Transfer of personal data to a third country or an international organization outside the European Economic Area (which includes the European Union, Liechtenstein, Iceland, and Norway) may take place in case there is an adequacy decision.

In the absence of such adequacy decision, the transfer to a third country may only take place in case the Supplying Data Controller, Receiving Data Controller has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

Personal data may only be transmitted if each Data Controller has given its prior written consent to such transmission.

Therefore, it is also important that instructions are given in case a transfer to a third country or an international organization should take place.

ARTICLE 13 : LIABILITY

Supplying Data Controllers declare that the processing activities subject to this Agreement are allowed from an ethical-legal perspective.

A Data Controller is liable for the damage caused by processing where it has not complied with obligations of the GDPR or, where he has acted outside or contrary to the Supplying Data Controllers conditions laid out in this Agreement.

ARTICLE 14 : DISSEMINATION OF RESULTS

The publication of any results and insights must take place in such a way that it is impossible to identify individual persons whose data has been used to generate these results and insights.

ARTICLE 15 : TERMINATION OF THE CONTRACT

In the event of breach of this Agreement or the GDPR, the Supplying Data Controllers concerned can instruct the Receiving Data Controllers concerned to stop further processing of the personal data with immediate effect when this would be reasonable and proportionate taking into account the severity of the breach.

This Agreement can be terminated by a Party with a period of a written notice of 2 months.

ARTICLE 16 : EXHAUSTIVENESS OF THE AGREEMENT

In the event that any one of these contractual clauses is found to be invalid in any way, the rest of the Agreement shall continue in full force. The Parties shall immediately seek to replace the contractual clause concerned with a valid contractual clause by amendment in writing which correctly represents the initial intentions of the Parties.

ARTICLE 17 : DATA DELETION AND RETENTION

Data deletion and retention shall be as described in the RECLAIM study protocol.

ARTICLE 18 : DATA BREACH NOTIFICATION

In case of any Personal Data Breach, a Processor shall, without undue delay, but no later than 24h after having become aware of the Personal Data Breach, notify the Controller(s) of the Personal Data Breach in writing by contacting the Controller's internal point of contact directly or the Data Protection Officer of the Controller(s). The contact details of the relevant person identified to receive the notification shall be communicated separately from the Controller to the Processor (e.g., by email).

This notification from the Processor to the Controller(s) should contain at least the following information:

i. The nature of the Personal Data Breach, which states the categories and (by approximation) the number of Data Subjects concerned, and stating the categories and (by approximation) the number of the Personal Data affected,
ii. The likely consequences of the Personal Data Breach, and
iii. A proposal for measures to be taken to address the Personal Data Breach, including (where appropriate) measures to mitigate any possible adverse effects of such Breach.

The Processor shall document (and shall keep such documentation available for the Controllers) any Personal Data Breaches, including the facts related to the Breach, its effects and the corrective measures taken. All reasonable actions shall be undertaken by the Processor to limit the (possible) adverse effects of Personal Data Breaches after consultation with the Controller(s) unless such consultation cannot be awaited due to the urgency, the scope and the nature of the Personal Data Breach.

Considering the nature of processing and the information available to the Processor, the Processor must assist the Controller(s) in ensuring compliance with the Controller's obligations related to the notification to the Supervisory Authority and the communication to Data Subjects of a Personal Data Breach, where required per applicable Data Protection Laws.

***

The signature of a representative of a Party received by electronic image transmission (such as portable document format) will constitute an original signature. Each Party receives a fully executed copy of the Agreement. Delivery of the fully executed copy by electronic image transmission shall have the same force and effect as delivery of the original Agreement.

ICOMETRIX NV

Name(s) – Wim Van Hecke

Title(s) – CEO

Read and acknowledged

General University Hospital Prague

Name(s) – Prof. Pavel Michálek, MD., Ph.D., D.E.S.A., M.Sc., MBA

Title(s) – Deputy for science, research and education

Read and acknowledged

Charité – Universitätsmedizin Berlin

Name(s) – Dr. Katharina Flemming

Title(s) – Head of Business Division Research Services

Read and acknowledged

Charité – Universitätsmedizin Berlin

Name(s) – Prof. Dr. Friedemann Paul

Title(s) – Director of the Experimental and Clinical Research Center (ECRC) at Charité

Read and acknowledged

Technische Universität Dresden

Name(s) – Katja Böttcher

Title(s) – Head of Unit, on behalf of the Chancellor

Read and acknowledged

Technische Universität Dresden

Name(s) – Prof. Dr. Tjalf Ziemssen

Title(s) – Project Leader

Read and acknowledged

Ruhr-Universität Bochum

Name(s) – Prof. Dr. med. Carsten Lukas

Title(s) – Head of the Institute of Neuroradiology, St. Josef Hospital, University Clinic of the Ruhr-University Bochum, Germany

Read and acknowledged

F. Hoffmann-La Roche

Name(s) – Vera Zingler MD, PhD, Neurologist

Title(s) – Global Medical Science Leader Healthcare Innovation & Medical Practice

Read and acknowledged

Bristol Myers Squibb

Name(s) – Jon Riolo

Title(s) – Director, Medical Affairs

Read and acknowledged

AB Science

Name(s) – Catherine Argillier

Title(s) – Head of Quality Assurance

Read and acknowledged

AALTO University Foundation sr.

Name(s) – Jouko Lampinen

Title(s) – Dean, School of Science

Read and acknowledged

Nocturne GmbH

Name(s) – Dr. Ella M. Kadas

Title(s) – CEO

Read and acknowledged

Azienda Socio Sanitaria Territoriale Papa Giovanni XXIII

Name(s) – Dr. Francesco Locati

Title(s) – General Manager

Read and acknowledged

Neuroquantic srl

Name(s) – Fabio Chiocchetti

Title(s) – Legal Representative

Read and acknowledged

APPENDIX 1 – NATURE AND PURPOSE

Nature and Purpose of the intended processing of personal data.

This Agreement covers the processing of the personal data for the purposes described in the "Clinical Impact through AI-assisted MS care: a retrospective multi-center observational study" protocol (study named RECLAIM).

For full details we refer to the RECLAIM study protocol and the CLAIMS grant application but in summary, we will collect, harmonize and make centrally available to the CLAIMS Consortium a retrospective dataset on people with Multiple Sclerosis, CIS, RIS, NMOSD and MOGAD for research purposes. This dataset will be used for the development, training, optimization and validation of novel biomarkers and AI-based diagnostic, prognostic and subtyping models to improve patient care, as well as for research purposes to enable the generation of insights on disease worsening and progression, patient prognosis, treatment decisions and responses and patient profiles of people with Multiple Sclerosis.

Data subjects

We will include retrospective data from patients from the five clinical partners (GUHP, RUB, TUD, CHARITE, PG23) and data from patients of clinical trials from the three pharmaceutical companies involved (ROCHE, BMS, ABSCIENCE). Patients must have a confirmed diagnosis of Multiple sclerosis, Neuromyelitis Optica spectrum disorder, Myelin oligodendrocyte glycoprotein antibody-associated disease, clinically isolated syndrome or, radiologically isolated syndrome.

Types of data collected

Category	Variables
Demographics	• Date of Visit / Reporting date • Date of Birth • (Biological) Sex • Country of Residence • Race / Ethnicity • Educational level • Employment Status • Smoking history • Smoking intensity • Family History of MS • Menopause present
Comorbidities	• Comorbidities • Date of comorbidity diagnosis • Type of comorbidity
Risk Factors	• Risk Factor • Date of Risk Factor diagnosis • Viral infections • Vitamin deficiency • Alcohol/Drug abuse • BMI > 30

Disease history	• Diagnosis • Date of diagnosis • Date of first manifestation • CSF and serum markers (e.g., Oligoclonal IgG bands) • If applicable: MS Course
Disease status	• Current signs and symptoms • EDSS • Functional systems scores • SDMT • T25FWT • 9-HPT • PASAT • Vibratory sense • Visual parameters • MSFC • PDSS • Several questionnaires to assess severity of symptoms and wider disease impact (e.g., economic).
Relapse	• Relapse event • Data of relapse • Steroid or other treatments for relapse • Hospitalisation • Recovery • Annualized relapse rate • Relapse type/site
Subclinical data	• Magnetic resonance imaging (MRI) from brain and spinal cord, including (but not limited to) T1-weighted scans, T2-weighted scans, FLAIR scans and SWI scans. • Optical coherence tomography (OCT) • Evoked potentials (EP) For each of these imaging modalities, the raw data will be centrally stored and analysed, and thereafter the analysis results and the accompanying meta data will be captured in the dataset.
Treatment history	• Start Date • Stop Date • Stop reason • Disease-modifying treatment (DMT), including dosage and frequency • Non-pharmaceutical treatment (NPT)

Place of the processing

Partner	Place of processing
icometrix NV	• AWS servers in Ireland (cloud storage) • Belgium
AALTO University Foundation sr.	Finland
Nocturne GmbH	• Germany (local installation) • AWS (planned) in Frankfurt (cloud installation)
Neuroquantic srl	• Italy (Microsoft cloud storage)

Sub-Processor

In the event that the data is communicated or accessible by a sub-processor, please identify the contact details of the sub-processor:

CLAIMS Partner	Third Party	Contact details
icometrix NV	**Amazon Web Services** (cloud storage and analysis) Avenue John F. Kennedy 38, LUXEMBOURG, 1855, LUXEMBOURG	https://aws.amazon.com/contact-us/
Nocturne GmbH	**Amazon Web Services** (cloud storage and analysis) Eschborner Landstraße 100, 60489 Frankfurt am Main, Germany	https://aws.amazon.com/contact-us/
Neuroquantic srl	**Microsoft cloud** (cloud storage and analysis) Microsoft: Strada Provinciale 415, 20090 Settala, Città Metropolitana di Milano, Italy	/

Contact details of the Data Protection Officer (DPO) of the data controllers

Partner	DPO	DPO email
General University Hospital Prague	/	poverenec@vfn.cz
Charité – Universitätsmedizin Berlin	Janet Fahron	datenschutzbeauftragte@charite.de
Technische Universität Dresden	/	dsv@ukdd.de
Ruhr-Universität Bochum	Andreas Koppenhagen	andreas.koppenhagen@kklbo.de
F. Hoffmann-La Roche	Florian Zabel	florian.zabel@roche.com
Bristol Myers Squibb	Jason Burns	eudpo@bms.com

AB Science	Catherine Argillier	dpo@ab-science.com
Nocturne GmbH	Ella M. Kadas	Ella.kadas@nocturne.one
icometrix NV	Riet de Kempeneer	dpo@icometrix.com
AALTO University	Anni Tuomela	dop@aalto.fi
Azienda Socio Sanitaria Territoriale Papa Giovanni XXIII	LTA srl	Regolamentoeuropeo@asst-pg23.it
Neuroquantic srl	/	fabio.chiocchetti@fiscalaudit.it admin@neuroquantic.com

APPENDIX 2 – TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

The Data Controllers should provide sufficient guarantees, in particular in terms of expert knowledge, reliability and resources, to implement technical and organizational measures as mentioned in article 32 GDPR which will meet the requirements of the GDPR, including for the security of processing (Recital 81 GDPR).

In order to ensure a level of security appropriate to the risk, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Data Controllers shall implement appropriate technical and organizational measures.

When assessing the appropriate level of security, the risks that are presented by processing should be taken into account, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.

ICOMETRIX

Appropriate technical and organisational measures are implemented to protect personal data against unauthorised or unlawful processing and against accidental loss, destruction or damage, as described in our quality manual. This includes:
• Pseudonymisation and encryption of personal data (see Cryptography, pseudonymization and anonymization of patient data, DICOM router 3.x pseudonymization)
• We ensure confidentiality, integrity, availability and resilience of processing systems and services through:
  ○ Internal, physical and electronic access control (see Access control, physical infrastructure management, clean desk and screen policy, visitor procedure, password requirements, antivirus and antimalware, e-mail policy, mobile device policy)
  ○ Isolation control (see Back-up system)
  ○ Monitoring (see IT infrastructure monitoring)
  ○ Data transfer control (see Personal information handling procedure)
  ○ Availability control (see Back-up system, antivirus and antimalware)
  ○ Rapid recovery (see IT infrastructure monitoring, Back-up system, Issue handling)
• We restore the availability and access to personal data in a timely manner in the event of a physical or technical incident by:
  ○ Availability control (see Back-up system, antivirus and antimalware)
  ○ Rapid recovery (see IT infrastructure monitoring, Back-up system, Issue handling)
• A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing is implemented by:
  ○ Data protection management (see Personal information handling procedure)
  ○ Incident response management (see Vigilance and incident reporting)
  ○ Data protection by design and by default (see Issue handling)
  ○ Agreement or contract control (see Information security user policy, Agreement on regulatory affairs responsibilities with third parties: checklist)
• Encryption (256 bit keys) for all computers and servers containing confidential data (more information in Cryptography);
• An automated back-up system (more information in Backup System);
• Protection against viruses and malware (more information in Antivirus and antimalware);
• An access control system that ensures that access to patient data are tightly restricted based on the concept of need-to-know (more information in Access control);

- Monitoring of the IT infrastructure, including capacity monitoring, availability monitoring, logfile monitoring, clock synchronization and vulnerability testing (more information in IT Infrastructure Monitoring);
- Prevention of unauthorized physical access (more information in Physical Infrastructure Management and Visitor procedure).

GUHP

Measures of pseudonymisation and encryption of personal data

- Only the data exporter (Institution) will have the key (Subject ID List) that links the subject ID with the actual patient record. This data is kept at the sites and is not transferred outside of the sites.
- Only pseudonymized data is transferred. The data is transferred in such a manner that the personal data cannot be attributed to a specific data subject, nor be used to single out the data subject in a larger group, without the use of additional information for de-identification which is kept separate from the pseudonymized data.

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

- Existence of formalized working instructions/procedures and appropriate training of employees and contractors
- Employees and contractors signed a written declaration to maintain confidentiality in accordance with the data protection law
- Implementation of a central identity management system
- Password procedures including frequency of their modification (e.g., length and complexity of password requirements, etc.)
- Implement a process for monitoring of information security and data protection.
- Automatic log-off in case of inactivity after defined time periods
- Access to backup data and media is restricted

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

- Existence of tested and documented back-up and recovery process
- Ensuring systems are functioning and that faults are reported

Ensuring stored personal data cannot be corrupted by means of a malfunctioning of the system

- Uninterruptible power supply (UPS)
- Business Continuity procedures
- Remote storage
- Anti-virus/ firewall systems

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing

- Password procedures (including special characters, minimum length, forced change of password)
- No access for guest users or anonymous accounts – role-based restriction of access to Personal Identifiable Information in relevant systems
- Central management of system access
- Access to IT systems subject to approval from HR Management and IT System Administrators
- Provide Air conditioning in server rooms

- Server rooms protected against fire, water and other physical damage

Measures for user identification and authorisation

- Differentiated access rights (profiles, roles, transactions and objects) to data and programs
- Identification of accessing persons (e.g., no multi-user accounts). Provide an enhanced user authentication process for remote system access from the Internet (e.g., 2-factor authentication using hardware token, etc.)
- Implementation of an enhanced user identification process (e.g., hardware token, biometric, etc.)
- Automatic blocking or timeout of workstation and/or User ID after incorrect access attempts

Measures for the protection of data during transmission

- Encryption of data in transit (i.e., transport encryption) using TLS 1.2 and AES 256-bit
- Sending of email to external recipients only in encrypted form (PGP, TLS, etc.). Use of digital signatures.
- Careful and regulated handling of portable storage media such as USB sticks, external hard drives, SD memory cards (e.g., encryption, storage in locked cabinets, etc.)
- Industry standard encryption of personal and confidential data when transferred through the internet (e.g., SFTP, https, VPN)
- Ensuring the establishment of an audit trail to document the transfer of personal and/or confidential data

Measures for the protection of data during storage

- Differentiated access rights (profiles, roles, transactions and objects) to data and programs
- Access rights defined according to duties
- Automatic log-off in case of inactivity after defined time periods
- Measures to prevent the use of automated data-processing systems by unauthorized persons using data communication equipment

Measures for ensuring physical security of locations at which personal data are processed

- Access control systems, e.g., ID reader, Smart card/transponder locking system
- Surveillance facilities - alarm system and camera recording of access
- Availability of Security staff, gatekeeper
- Employee identification badges/visibility of such
- Control or monitor personnel (including third parties) who access secure areas
- Physical hardware protection (e.g., door locking, lockable racks, etc.)

Measures for ensuring events logging

- Logging user activities on IT systems
- Ensuring the establishment of an audit trail to document whether and by whom personal data have been entered into, modified in, or removed from personal data processing systems (entry control). Protect log files against unauthorized use and modification.

Measures for ensuring system configuration, including default configuration

- Unambiguous wording of contractual instructions
- Monitoring of contract performance

Measures for internal IT and IT security governance and management

- Restriction of access to data stored for different purposes according to staff duties
- Separation of business IT systems
- Separation of IT testing and production environments

- Roles and authorizations process: administrator, reviser, user, etc.

Measures for certification/assurance of processes and products

- Existence of formalized working instructions/standard operating procedures and appropriate training of employees and contractors

Measures for ensuring data minimisation

- Data collected in the Case Report Form is minimized to data required as per the trial protocol only
- The type and amount of Personal Identifiable Information data transferred is strictly the minimum necessary to meet the consented purpose, in line with the law of the data subject's country of residence

Measures for ensuring data quality

- Regular (monthly) checks of imported data per Data Management Plan

Measures for ensuring limited data retention

- Clinical records (eTMF and ISFs) will be retained according to the Retention period defined in the Clinical Trial Directive (at least 25 years). After the retention period, the data will be fully anonymized or deleted.
- The data will be kept by Importer for 15 years or as per applicable laws.

Measures for ensuring accountability

- Implementation of a workflow to process sensitive data.
- Ensuring the establishment of change control and separation of duties processes in-place to protect sensitive data from unauthorized changes

Measures for allowing data portability and ensuring erasure

- Use of available technology to allow data portability and data erasure in accordance to data subject's rights or legal obligation

AALTO

Servers are hosted in data centres with top-tier providers that respect strict control for physical access to their servers, including but not limited to:

- video surveillance
- intrusion detection systems
- two-factor authentication for authorized staff

The system is protected against security breaches and network attacks. The system is protected ag ainst injection attacks and other known data security threats.

Receiving Data Controller protects against system intrusions and network attacks and monitors system security and intrusion attempts. The security updates for the software components are installed regularly and quickly enough.

The information security of the system has been extensively tested. Receiving Data Controller pledges to provide a test report upon request.

Receiving Data Controllers' maintenance and system administrators have personal accounts and passwords in use.

The system prevents unintentional disabling of security functions. Only superusers have the right to disable security functions e.g., in case of troubleshooting.

Receiving Data Controllers 's systems and operational procedures ensure the secure administration of local user accounts and passwords. Passwords are stored in the systems encrypted with strong one-way hashing functions and salted. The system does not include functions that can be used to by-pass the built-in password control or decode user passwords. Not even the system's main administrator should be able to retrieve the password (local user accounts, authentication traffic).

Receiving Data Controllers systems have mechanisms to prevent automated login attempts. The login to the system or through the system is possible only with a certificate issued by established and recognized certificate authority (CA) and using an encrypted connection.

The network traffic for Service providing must use at least AES-128 TLS 1.x encryption and must be encrypted by certificate of an established and recognized certificate authority (CA).

Files containing personal, confidential or sensitive data cannot open without system logging.

The data in the system cannot be modified without leaving traces in the system logs and monitoring mechanisms. E.g., the database data cannot be modified (addition, search, change and deletion of data) without a system login.

The system provides ways to audit, update and remove old or faulty data.

Receiving Data Controllers data is not mixed up with data of a third party and that any third party is not able to access the data.

The remote maintenance is implemented from a security point of view:

- the connections can be limited to specified allowed sources
- the maintenance is not possible without a user identification and authentication
- the maintenance traffic of information is separated and encrypted

The systems can be configured to produce at least the following reports: security exceptions, attempted and successful logins, attempted and successful elevations of rights.

CHARITE

Charité complies with applicable foreign and domestic laws and regulations as amended from time to time, including without limitation those governing the protection of human subjects (including without limitation the International Conference on Harmonisation Good Clinical Practice standards), and concerning privacy and data protection including without limitation the privacy and security standards established under applicable law. In addition to the General Data Protection Regulation (GDPR), state regulations such as the State Data Protection Act (BlnDSG) and the State Hospital Act (BlnLKG) apply to the Charité - Universitätsmedizin Berlin. The data security concept in force at the Charité's study center, Experimental and Clinical Research Center, can be requested from the Charité as clinical coordinator of CLAIMS.

The following provides an overview of the most important technical and organizational aspects implemented to protect personal data against unauthorised or unlawful processing, accidental loss and destruction or damage:

- For scientific projects/clinical trials, the participants must give consent to data collection and processing with the corresponding study purpose.
- Prohibition of transfer of sensitive data to third parties, unless explicitly stipulated by contract, commitment of employees to data secrecy and confidentiality
- The Data Protection & Governance Division of the Charité Universitätsmedizin Berlin will be involved in the event of breach or subject complaints to institution with respect to data protection issues and claim of rights such as requests for information about stored data or withdrawal of consent. It will also be involved in requests from data protection supervisory authorities

- Regular training of the staff on data protection and security (once per year)
- Pseudonymisation of personal data
    - Personal data is collected and securely stored in patient or test subject files and clinical workstations for MRI and visual examinations. These data are converted into study data through pseudonymization and transferred to the Charité-run Phoenix PACS platform for archiving.
    - Clinical data are collected on CRF or in patient health records. Study data are documented in pseudonymised form in an EDC system (REDCap) and stored there.
- Anonymization of personal data after 10 years of storage for research purposes if applicable according to participant consent
- Data separation requirement
    - Identification codes are recorded together with the identifying data of the participants in a central list (participant identification list/Log-List)
    - Restricted access to Log-Lists → without access to this list, pseudonymized patient data cannot be linked back to original patient
- Access and access control
    - Restricted and password-protected server access
    - Restricted access to study data (user authentication for EDC system, restricted data export rights)
    - Restricted access to data saved on clinical workstations for EMR, MRI and visual examinations
    - Prevention of unauthorized physical access by restricted access to premises, controlled key allocation to authorized persons
    - Alarm systems, secure door locks
    - Withdrawal of access rights if necessary
- Secure data transfer
    - No identifying data is shared, pseudonymized study data is only shared with authorized cooperation partners in accordance with participant consent and contractual arrangements
    - Suitable transfer will be coordinated involving responsible divisions of Charité – Universitätsmedizin Berlin
    - The transfer of personal data to private devices or systems is technically and/or organizationally prohibited.
    - Appropriately encrypted transmission of electronic data according to the state of the art.
- Integrity control:
    - Personal data (concerning participant files as well as screening and participant identification lists) are regularly checked for plausibility and completeness and corrected and/or supplemented if necessary.
    - Monitoring of the clinical data for internal quality control
    - Internal protocols for documentation control
        - EDC-System audit trails
        - In documents that are kept on paper, entries, changes and deletions are marked with the employee's personal name abbreviation.
- Regular, automated backups of study data are routinely carried out by the IT division
- Regular software updates by trained staff
- Network infrastructure and workstations security
- Secure data deletion

Secure overwriting/final deletion of the data records and removal of any backup copies. If that is not possible/intended: anonymization. The measures are primarily intended to ensure compliance

with the principles of confidentiality, transparency, data integrity, legality, purpose limitation, data minimization, non-linkability and authenticity.

NOCTURNE

Nocturne has implemented appropriate technical and organizational measures to protect personal data from unauthorized processing, damage, or loss. The following points outline the security measures in place:

- Pseudonymization: Before uploading to the planned AWS server, we employ pseudonymization on personal data, with corresponding pseudonymized tags persisting locally on the device from which the data is uploaded. For the local installation option, the data undergoes the data supplier's security measures regarding data safety and security. All measures implemented by Nocturne ensure and safeguard that no data is leaked or uploaded to any external server.
- Zero-knowledge: Within the cloud service, zero-knowledge techniques are employed to uphold user data confidentiality through access control and additional data encryption measures. In the local installation, the system is allocated to a specific user and protected by a user-password authentication mechanism. Furthermore, we ensure secure data transfer by using transmission data encryption.
- Data backup and restoration: We ensure the prompt restoration of availability and access to personal data in the event of a physical or technical incident.
- Secure data transfer: We implement secure data transfer in compliance with German law regulations, following guidelines and requirements. An automatic backup system is also in place.
- Access Control: We implement multi-level authentication in conjunction with user-password protocols to prevent unauthorized access. For local installations, we rely solely on user-password authentication, given the additional authentication layer already provided by the data supplier.
- Quality Control: Integrated into the quality management system are:
    - Data protection and data safeguard management
    - Incident response management (Vigilance and incident reporting)
    - Security, Safety, and Risk policies
    - Agreement on regulatory affairs responsibilities with third parties (contract)
- IT System Monitoring: This involves:
    - Assessing the utilization of resources such as CPU, memory, storage, and network bandwidth
    - Tracking uptime, downtime, and response times for critical components
    - Analysing system and application logs to detect abnormal patterns, errors, or security incidents
    - Implementing synchronization mechanisms to maintain accurate time across the infrastructure
    - Conducting regular vulnerability assessments to identify security gaps in software, configurations, or network infrastructure.
    - Data Encryption: The personal data of users undergoes encryption at two distinct levels—prior to uploading and on the server—to ensure robust security and prevent any potential data leakage or tracing of personal information.
- Data Deletion: We guarantee the deletion of uploaded data after processing, adhering to the user's consent. Additionally, we maintain comprehensive transaction logs for subsequent review purposes.

RUB

RUB and St. Josef Hospital Bochum, University Clinic of RUB, complies with applicable foreign and domestic laws and regulations as amended from time to time, including without limitation those governing the protection of human subjects (including without limitation the International Conference on Harmonisation Good Clinical Practice standards), and concerning privacy and data protection including without limitation the privacy and security standards established under applicable law.

Technical and organizational aspects implemented to protect personal data against unauthorised or unlawful processing, accidental loss and destruction or damage:

Clinical trials / scientific projects:

- For scientific projects/clinical trials, the participants must give consent to data collection and processing with the corresponding study purpose.
- Sensitive data must not be transferred to third parties, unless explicitly stipulated by contract.
- Employees are committed to data secrecy and confidentiality.
- Pseudonymisation of personal data: Personal data is collected and securely stored in patient files in the clinics information system (Dedalus-ORBIS). MRI data are stored in the clinics picture archiving system (VISUS-PACS). Data are converted into study data through pseudonymization. Access to the key file linking the pseudonymisation IDs and patient IDs is strictly limited to study personnel, and password protected.

Access and access control:

- Restricted and password-protected server access
- Restricted access to study data
- Prevention of unauthorized physical access by restricted access to premises, controlled key allocation to authorized persons
- Alarm systems, secure door locks

Secure data transfer:

- No identifying data is shared, pseudonymized study data is only shared with authorized cooperation partners in accordance with participant consent and contractual arrangements
- The transfer of personal data to private devices or systems is technically and/or organizationally prohibited.
- Appropriately encrypted transmission of electronic data according to the state of the art (e.g., SFTP, https, VPN).

Network/Server infrastructure and security:

- Differentiated access rights of users (profiles, roles, transactions and objects) to data and programs
- Access rights defined according to the duties of the employees
- Automatic log-off in case of inactivity after defined time periods; empty desktop policy
- Password procedures (including special characters, minimum length, forced change of password_
- Existence of tested and documented back-up and recovery process
- Uninterruptible power supply (UPS)
- Business Continuity procedures
- Remote storage of backups
- Anti-virus/ firewall systems

NEUROQUANTIC

NeuroQuantic has implemented adequate measures to protect personal data from unauthorized processing, damage, or loss. In particular:

- Pseudonymization: As Neuroquantic will handle data already anonymized before their uploading to the allocated server, no sensitive data will be processed. All measures implemented by NeuroQuantic ensure and safeguard that no data is leaked or uploaded to any external server.
- Data backup and restoration: prompt restoration of availability and access to personal data in the event of a physical or technical incident.
- Secure data transfer: implemented in compliance with Italian law regulations, following guidelines and requirements and through procedures agreed upon with Claims Data Management. An automatic back-up system is in place.
- Access Control: User-password protocols to prevent unauthorized access.
- Quality Control:
    - Data protection and data safeguard management
    - Incident response management
    - Security, Safety, and Risk policies
    - Agreement on regulatory affairs responsibilities
- IT System Monitoring involving:
    - Assessing and restricting the use of resources such as CPU, memory, storage, and network bandwidth
    - Analysing system and applications, including in-house software, to detect abnormal patterns, errors, or security incidents
    - Conducting regular monitoring to security gaps in software, configurations, or network infrastructure.
- Data Deletion: NeuroQuantic guarantees the deletion of uploaded data after processing. According to the present DPA, copy of the personal data will be destroyed after a period of maximum 2 years after the Project has ended.

PG23

Technical and organizational aspects implemented to protect personal data against unauthorised or unlawful processing, accidental loss and destruction or damage:

Clinical trials / scientific projects:

- For scientific projects/clinical trials, the participants must give consent to data collection and processing with the corresponding study purpose.
- Sensitive data must not be transferred to third parties, unless explicitly stipulated by contract.
- Employees are committed to data secrecy and confidentiality.
- Pseudonymisation of personal data: Personal data is collected and securely stored in patient files in the clinics information system. MRI data are stored in the clinics picture archiving system (PACS). Data are converted into study data through pseudonymization. Access to the key file linking the pseudonymisation IDs and patient IDs is strictly limited to study personnel, and password protected.

Access and access control:

- Implementation of a central identity management system
- Differentiated access rights (profiles, roles, transactions and objects) to data and programs

- Password procedures including frequency of their modification (e.g., length and complexity of password requirements, etc.)
- Automatic log-off in case of inactivity after defined time periods
- Restricted and password-protected server access
- Restricted access to study data
- Prevention of unauthorized physical access by restricted access to premises, controlled key allocation to authorized persons

Secure data transfer:

- No identifying data is shared, pseudonymized study data is only shared with authorized cooperation partners in accordance with participant consent and contractual arrangements
- Appropriately encrypted transmission of electronic data according to the state of the art (e.g., SFTP, https, VPN).

Network/Server infrastructure and security:

- Existence of tested and documented back-up and recovery process
- Uninterruptible power supply (UPS)
- Business Continuity procedures
- Provide Air conditioning in server rooms
- Server rooms protected against fire, water and other physical damage
- Anti-virus/ firewall systems.

ATTESTAZIONE DI REGOLARITA' AMMINISTRATIVO-CONTABILE (proposta n. 1484/2025)

Oggetto: AUTORIZZAZIONE ALL'AVVIO DELLO STUDIO RECLAIMS (REG. 0179-2025) PRESSO LA SC NEUROLOGIA DI CUI È PROMOTORE CHARITÈ – UNIVERSITÄTSMEDIZIN BERLIN.

SC PROPONENTE

Si attesta la regolarità tecnica del provvedimento, essendo state osservate le norme e le procedure previste per la specifica materia.

Si precisa, altresì, che:

A. il provvedimento:

☐ prevede
☒ non prevede

COSTI diretti a carico dell'ASST

B. il provvedimento:

☐ prevede
☒ non prevede

RICAVI da parte dell'ASST.

Bergamo, 27/08/2025

Il direttore

Dr. / Dr.ssa Monia Maria Beatrice Lorini

PARERE DIRETTORI

all'adozione della proposta di deliberazione N.1484/2025
ad oggetto:
AUTORIZZAZIONE ALL'AVVIO DELLO STUDIO RECLAIMS (REG. 0179-2025) PRESSO LA SC NEUROLOGIA DI CUI È PROMOTORE CHARITÈ – UNIVERSITÄTSMEDIZIN BERLIN.

Ciascuno per gli aspetti di propria competenza, vista anche l'attestazione di regolarità amministrativo-contabile.

DIRETTORE AMMINISTRATIVO : Ha espresso il seguente parere: X FAVOREVOLE NON FAVOREVOLE ASTENUTO	Vecchi Gianluca
Note:	

DIRETTORE SANITARIO Facente funzione: Ha espresso il seguente parere: X FAVOREVOLE NON FAVOREVOLE ASTENUTO	Locati Francesco Angelo
Note:	

DIRETTORE SOCIOSANITARIO : Ha espresso il seguente parere: X FAVOREVOLE NON FAVOREVOLE ASTENUTO	Cesa Simonetta
Note:	

CERTIFICATO DI PUBBLICAZIONE

Pubblicata all'Albo Pretorio on-line
dell'Azienda socio sanitaria territoriale
"Papa Giovanni XXIII" Bergamo

per 15 giorni
