EORTC European Organisation for Research and Treatment of Cancer The future of cancer therapy	**Policy on Protection of Personal Data**		
Document owner	Data Protection	Version number	1.0
Effective date	2024-12-24	Identifier	P-01-POL-01

1 Purpose

This policy describes how EORTC processes personal data in accordance with data protection laws and ensures compliance with all applicable legal obligations.

2 Scope

This policy applies to all personal data collected, stored, or processed by EORTC staff (employees or contract workers), its members or executives, experts and any other third party (including but not limited to partners, vendors, contractors and their relevant members or staff) handling personal data on behalf of EORTC or otherwise related to its activities. Exceptions include:

- Processing of anonymous data;
- Personal or household activities, as defined in GDPR Article 2(2)(c);
- Data of deceased individuals, unless otherwise specified by law, provided it does not contain information about living persons (e.g. family members).

This policy governs the use of personal data on all EORTC-owned or leased hardware, including EORTC-owned, licensed, or supported data and programs, as well as any data and programs provided by third parties. It also covers data stored at remote locations or in cloud-based systems. The policy applies to personal data stored in structured filing systems, whether in digital or paper format, used for EORTC activities.

3 Policy statement

Within the scope of this policy, any data collection, storage or processing shall comply with:

- Declaration of Helsinki
- EU General Data Protection Regulation
- Belgian law of 30 July 2018 on the protection of natural persons with regard to the processing of personal data

When acting as a data processor, joint controller, or handling data from outside the EU, EORTC shall ensure adherence to relevant national or international laws (e.g., GDPR, UK GDPR, FADP, HIPAA). As a data processor, EORTC will act in accordance with the instructions provided by the data controller, provided such instructions do not infringe the

GDPR or other applicable laws. Such adherence is ensured through the involvement of appropriate legal and compliance expertise. Applicable laws and responsibilities shall be reviewed and communicated, and EORTC staff involved in such projects are informed prior to the start of processing.

4 Changes since last version

Process step	**Changes since last version**
ALL	Superseding POL021 v 2.0: Protection of Personal Data
Scope	Clarified scope for cloud-based systems, personal/household activities, and structured filing systems.
Policy Statement	Added compliance with Belgian Law of 30 July 2018, UK GDPR, FADP, and HIPAA, etc.
Key Principles	Enhanced accountability, data minimization, accuracy, and breach notification procedures.
Data subjects and their rights	Simplified content, clarified contact procedures for data subjects.
Privacy by Design	Expanded DPIA requirements and integration of privacy by design.
Data Protection Representatives	Added Data Protection Representatives (DPRs) in the UK and Switzerland.
Engagement of Processors	Strengthened requirements for engaging data processors, including Data Processing Addendum (DPA).
Data Breaches and Notifications	Added breach response and notification process.
Collaboration Outside EU	Added compliance measures for non-EU collaborations and data sharing.

5 Policy

5.1 Key principles

Within the scope of this policy, EORTC ensures compliance with the following data protection principles, as outlined in the GDPR:

- **Lawfulness, fairness and transparency of the processing:** Personal data is processed fairly, lawfully, and transparently. EORTC shall establish a valid legal basis for each processing activity as data controller, as per GDPR Article 6, and document the basis in the records of processing activities.
- **Purpose limitation:** Personal data is collected and processed only for specified, explicit, and legitimate purposes. Further processing shall not occur unless compatible with the original purpose, in line with GDPR Article 5(1)(b).
- **Data minimization and accuracy:** EORTC ensures that personal data is accurate, adequate, relevant, and limited to what is necessary for the purpose. Inaccurate data shall be corrected or deleted promptly, as per GDPR Article 5(1)(c) and (d).
- **Limited retention of personal data:** Personal data shall not be retained for longer than necessary. Retention periods are defined per EORTC procedures, with regular reviews in cases where retention depends on events.
- **Security and confidentiality:** EORTC applies appropriate technical and organizational measures to safeguard personal data against unauthorized processing, loss, or damage. Procedures are in place for reporting potential data breaches or unauthorized disclosures, and failure to report such incidents may result in disciplinary action.
- **Accountability:** EORTC takes responsibility for compliance with all data protection principles and is able to demonstrate this compliance, as required by GDPR Article 5(2). Internal audits are conducted by EORTC to ensure adherence to this policy.

5.2 Data subjects and their rights

Applicable data protection laws grant data subjects specific rights. The rights of data subjects involved in EORTC's processing activities, along with the process for exercising these rights, are detailed in the Privacy Notice provided to them in the context of the processing activities that they are involved in.

To exercise their rights or file a complaint:

- Patients (and/or caregivers) shall contact their study doctor ("investigator") or hospital using the contact information provided to them.
- All other individuals may contact the EORTC Data Protection Officer (DPO) at dpo@eortc.org.

EORTC addresses all requests and complaints in compliance with applicable data protection regulations.

5.3 Privacy by design and data protection impact assessments

EORTC follows the principle of privacy by design, ensuring that data protection is embedded into all processes from the onset. Data protection impact assessments (DPIAs) are conducted in accordance with GDPR Article 35 when processing is likely to result in a high risk to the rights and freedoms of individuals, such as when introducing new technologies, processing sensitive data, or transferring data internationally.

EORTC maintains and regularly updates legal, organizational, and technical measures, including contracts, policies, IT security protocols, and more, to ensure data protection is integrated throughout the entire lifecycle of any project, process or system involving personal data, from planning to data destruction or anonymization.

5.4 Data protection officer (DPO)

Due to the nature of EORTC's core activities, which involves the large-scale processing of special categories of personal data, including health and genetic data, EORTC has appointed a data protection officer (DPO). The data protection officer advises on and monitors compliance with applicable data protection laws and this policy and can be contacted at dpo@eortc.org.

5.5 Awareness and training

EORTC ensures that all its personnel receive training on this policy and the applicable data protection laws relevant to their function.

5.6 Data protection representative

Since EORTC operates outside of certain jurisdictions, it has appointed data protection representatives (DPR) in the UK and Switzerland. The data protection representatives act as the point of contact for data protection matters in these regions. Should you need further information about EORTC’s DPRs, please contact our DPO.

5.7 Engagement of processors

EORTC only engages data processors that provide sufficient guarantees that their systems and practices comply with applicable data protection laws. Data processors are engaged through an agreement containing appropriate data privacy provisions that adheres to the requirements of relevant data protection laws and any applicable contractual obligations, provided these do not contradict legal requirements.

5.8 Supervisory authority

EORTC's headquarter is located in Belgium, making the Belgian Data Protection Authority its supervisory authority. EORTC, along with its personnel and data protection representatives, fully cooperate with the authority upon request, including during any inspections or inquiries.

5.9 Records of processing activities

EORTC maintains records of all processing activities it conducts, whether as a controller (alone or jointly with others) or as a processor, in compliance with GDPR Article 30. These records are kept up to date and available for inspection by supervisory authorities.

5.10 Data breaches and notifications

In the event of a personal data breach, EORTC promptly assesses the risk to the rights and freedoms of data subjects. If required, EORTC notifies the relevant data protection authorities within 72 hours, in accordance with GDPR Article 33, and informs affected data subjects without undue delay, as per GDPR Article 34. EORTC has established a process to manage the assessment, notification, and response to data breaches to ensure compliance with applicable regulations. All data breaches are documented centrally for tracking and compliance purposes.

5.11 Sharing of data and Scientific Research Processing

EORTC ensures the protection of personal data when transferred to other organizations, especially across international borders, in compliance with data protection laws and applicable safeguards.

Certain data subject rights may not apply to personal data processed for scientific research under specific exemptions in data protection laws. Personal data may be retained for longer periods if used solely for scientific purposes, provided appropriate safeguards are in place. Once no longer needed for its original purpose, personal data is deleted or anonymized, unless this is impossible or would require disproportionate effort.

EORTC may reuse previously collected data sets for new research, but only if such reuse is permitted under applicable laws. Reuse of data for purposes incompatible with the original collection is treated as a new processing activity and requires separate legal justification.

5.12 Collaboration and sharing of data Outside the EU

When collaborating with partners or sharing data outside the EU, especially when sharing with countries which are not recognized by the EU as adequate, EORTC takes all reasonable efforts to ensure compliance with applicable local laws in other regions.

EORTC collaborates with partners in regions such as the U.S. and other non-European territories, relying on these partners to comply with local privacy requirements. Before engaging in cross-border data sharing or collaboration, EORTC shall assess the legal

requirements of the target jurisdiction and ensure appropriate safeguards are in place. This may include entering into agreements that incorporate Standard Contractual Clauses (SCCs), assessing the adequacy of data protection in the destination country, or implementing additional security measures.

6 Definitions

- **Controller:** The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law. (Art. 4 GDPR, definition 7)
- **Data Privacy Agreement:** To document agreement between sponsor and site staff (e.g., national or regional data privacy requirements); often contained in Clinical Trial Agreement (TMF Reference Model)
- **Personal data:** any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. (Art. 4 GDPR, definition 1)
- **Processing:** Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction (Art. 4 GDPR, definition 2)
- **Processor:** a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. (Art. 4 GDPR, definition 8)
- **Supervisory authority:** an independent public authority which is established by a Member State pursuant to Article 51 GDPR. (Art. 4 GDPR, definition 21)

7 References

- Universal declaration of Human rights (art 12)
- EU data protection regulation 2016/679
- European Convention on Human Rights (art 8)
- European charter on patient rights
- Declaration of Helsinki
- Guideline for Good Clinical Practice E6 ICH-GCP E6
- Loi du 26 fevrier 2003 modifiant la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel et la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-Carrefour de la securité sociale en vue d'aménager le statut et d'étendre les compétences de la Commission de la protection de la vie privée.
- Royal Decree of 13 February 2001 providing further details to the Belgian Law of 30 July 2018 on the protection of natural persons with regard to the processing of personal data

8 Signature

This document will be electronically signed.
The signatories acknowledge that electronic signature is legally binding and equivalent to a handwritten signature.

Author Xiao Liu Data Protection Officer	Signed by: Xiao Liu Signer Name: Xiao Liu Signing Reason: I am the author of this document Signing Time: 03 December 2024 | 11:15:58 CET 0AB9ACC44A6A410DA69FB1D63D945034
Approved & authorized by Denis Lacombe Chief executive officer *On behalf of the Board*	Signed by: Denis Lacombe Signer Name: Denis Lacombe Signing Reason: I approve this document Signing Time: 03 December 2024 | 15:44:26 CET 457339F472784605806FBD4D54FBD7A4