EORTC
European Organisation for Research and Treatment of Cancer
The future of cancer therapy

Avenue E. Mounier 83/11
1200 Brussels
Belgium
Tel: +32 2 774 1611
Email: eortc@eortc.be
www.eortc.org

Protection of Personal Data

POL021

Version 2.0

ALWAYS REFER TO THE INTRANET TO CHECK THE VALIDITY OF THIS DOCUMENT

Author *Head International Policy Office* Anastassia Negrouk	Signature:	Date: (ex: 10-Feb-2017)
Authorized by: *Director General* *On Behalf of the Board* Denis Lacombe	Signature:	Date: (ex: 10-Feb-2017)

Table of Contents

1 PURPOSE

EORTC legitimate mission is to coordinate and conduct throughout its network and in collaboration with third parties, international prospective and retrospective translational and clinical research to improve the standard of cancer treatment for patients. Aside this primary mission, EORTC also develops and improves research methodologies and tools and organizes educational events and courses. Last, but not the least, EORTC also raises funds to support its activities.

This policy describes how EORTC ensure protection of personal data it processes as a data controller and as a data processor.

2 DEFINITIONS

- **Personal data**: any information relating directly or indirectly to an identified or identifiable natural person
- **Health data:** personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status
- **Anonymous data**: data which does not relate to an identified or identifiable natural person; or personal data rendered anonymous in such a manner that the data subject is not or no longer directly or indirectly identifiable
- **Pseudoanonymised data**: data which can no longer directly be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data cannot be attributed to an identified or identifiable natural person
- **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
- **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 and to whom the Personal data is pertains
- **Data 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
- **Data processor**: a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller
- **Supervisory Authority**: an independent public authority, which is established by a Member State. In the scope of this document: Belgian Privacy Commission

3 POLICY

3.1 COMPLIANCE

Within the scope of this policy any data collection, storage or processing shall comply with:
- relevant parts of the Universal declaration of Human rights, the European Convention on Human Rights and the European charter on patient rights
- Declaration of Helsinki
- principles of ICH GCP
- relevant recommendation of Working Party 29 / European Data Protection Board
- EU General Data Protection legislation (REGULATION (EU) 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, and repealing Directive 95/46/EC).
- Belgian law(s) on data protection and any relevant recommendation of Belgian Privacy Commission
- other national privacy laws when applicable

In situations where EORTC would handle the data on behalf of another party (as data processor) or work in collaboration with other parties (as joint controllers) or otherwise collect data from outside EU, other national (Swiss data protection law, HIPPA etc…) or international legislations may apply. If this is the case, relevant contracts shall specify the law applicable and EORTC staff involved in those projects shall be informed prior to the start of relevant processing.

3.2 SCOPE

This policy applies to any personal data collected, stored or processed or otherwise handled by EORTC staff (employees or external workers), its members or executives, experts or 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, with following exceptions:

- this policy does not apply to the processing of anonymous data;
- unless otherwise specified by law applicable in a specific case, this policy does not apply to data of deceased subjects insofar as it does not contain any data about other data of living subjects (e.g. family members).

This policy relates among others to their use of any EORTC-owned hardware (and those leased by or rented or on loan to EORTC), centrally managed or otherwise; to all EORTC-owned, licensed or otherwise supported data and programs (wherever stored); and to all data and programs provided to EORTC by third parties (wherever stored). The policy also relates to personal data contained in any structured filing system created for the purposes of EORTC business, including paper files and records of any structured format.

4 KEY PRINCIPLES OF PERSONAL DATA PROTECTION

Within the scope of this policy all following principles will apply:

4.1 Lawfulness, fairness and transparency of the processing

Any personal data processed by EORTC or under its responsibility, are processed fairly, lawfully and in a transparent manner.

4.2 Purpose limitation

Any personal data collected by EORTC or under its responsibility, are collected only for specified, explicit and legitimate purposes and do not further process it in a way incompatible with those purposes (clinical research performed in compliance with applicable legislation is not incompatible with initial purposes).

4.3 Data minimization and accuracy

EORTC, as either, data controller or data processor, ensures that personal data is:
- accurate and kept up-to-date;
- adequate, relevant and not excessive in relation to the purpose for which the personal data was collected and processed.

4.4 Limited retention of personal data

EORTC ensures personal data that are processed by EORTC or under its responsibility are not kept longer than is necessary for the purpose(s) for which the personal data are processed.
However, different types of data have different retention periods. EORTC has a procedure in place describing the adequate retention period of each type of data. Where retention period cannot be defined as a fixed number of years, but is event dependent, the review of adequacy of further retention is performed regularly (yearly for staff related data, every 3 years for professional contacts and every 5 years for research subject data).

4.5 Security and confidentiality

EORTC implements appropriate technical and organizational measures to protect personal data against unauthorised or unlawful processing and against accidental loss, destruction or damage (including, but not limited to processing by sub-contractors).
EORTC has procedures in place to ensure its staff and sub-contractors promptly report any suspicion of breach to data privacy or any unauthorized disclosure, deletions, losses or any other type of non-authorized processing of personal data.
After appropriate evaluation, EORTC DPO takes relevant actions, including immediate reporting to the data controller (when EORTC is data processor) or reporting of confirmed relevant data breaches to EORTC's supervisory authority (when EORTC is data controller) in compliance with standard operating procedures in place.
Negligent loss or unauthorized disclosure of personal data, or failure to report such events, may be treated as a disciplinary matter and could be considered gross misconduct.
EORTC Quality Assurance ensures compliance with this policy while conducting internal audits as per its standard operating procedures.
In addition, EORTC ensures, including by appropriate training and instruction, that:

- any software, electronic tools or devices are designed, set-up and maintained in a way that provides sufficient level of security to personal data processed by EORTC in compliance with applicable legislation in the domain of data security and any other security norm as applicable to each treatment;
- any software, electronic tool or devices operates in such a way that ensures personal data are being processed in a way that enables their authenticity, reliability and usability and are capable of speedy and efficient retrieval;
- appropriate systems are in place to prevent unauthorized access, disclosure and loss;
- personal data are not transferred outside EU without adequate protection and/or adequate safeguards in place;

- systems ensure data are archived or disposed securely and confidentially for the entire duration of archiving as required by applicable legislation.

5 DATA SUBJECTS AND THEIR RIGHTS

5.1 Data subjects

EORTC processes personal data relating to (non-exhaustive list):

5.1.1 EORTC staff

- “EORTC employees”: Employees of EORTC (current and former employees) and their relatives/immediate family members.
- “External workers”: Any individuals, who are not EORTC employees but who provide services under a contract or similar agreement for or on behalf of EORTC, including contractors, independent consultants, students, fellows and interim workers.
- "Candidates": Individuals seeking position within EORTC, weather as employee, expert or fellow.

5.1.2 EORTC professional contacts

- “Healthcare professionals”: Any individuals who are professionally engaged in diagnosis, treatment, and delivery of healthcare, including, but not limited to, physicians, physician assistants, nurses, pharmacists, researchers, staff of clinical laboratories and biobanks, medical or any other staff of healthcare facilities; EORTC experts, members and executives.
- "Government officials": Any individual representing regulatory and/or governmental bodies related on the national and/or EU level, including but not limited to members of EU commission, EU or national parliaments and councils, ministries, drug agencies and payers.
- “Partners and vendors”: Employees and legal representatives of EORTC partners, vendors providing services and/or products to EORTC, including, but not only industry, consulting firms, Contract Research Organizations (CROs), external laboratories and biobanks (other than those of healthcare institutions), distributors.
- "Donors": individuals or employees and legal representatives of organizations donating or that could potentially donate funds to support EORTC activities.
- "Event participants": individuals interested to participate to events and courses organized or co-organized by EORTC.
- "Requestors of information": individuals addressing questions to EORTC through its web site or by other means (outside requests in the scope of exercise of data subjects' rights).
- "Other professional partners" individuals, employees, or legal representatives of any partner or subcontractor professionally engaged with EORTC and different from all of the categories above (can include patient advocates).

5.1.3 Research participants

- “Patients and caregivers”: Cancer patients and their relatives/family members as well as caregivers
- "Other research participants": research participants who are not cancer patients

5.2 Data subject's rights

EORTC processes personal data in a way that respects data subject's rights (unless specific exemptions apply as per applicable legislation (1)):

- right to be informed
- right of access
- right of rectification
- right of erasure
- right to data portability
- right to object
- right to restriction of processing and to objection to further processing
- right to file a complaint with their data protection authority

To exercise their rights or to file a complaint (in case subject believe that their personal information has been processed in violation of applicable legislation), patients (and/or caregivers) shall contact their study doctor ("investigator")/ hospital using contact details they are provided with.
All other individuals can write to the EORTC DPO to exercise their rights or to file a complaint, by sending an email to: DPOatEORTC.be. EORTC will investigate the request/complaint within the delays imposed by regulation.

6 PRIVACY BY DESIGN AND DATA PROTECTION PRIVACY IMPACT ASSESSMENT

EORTC applies the principle of privacy by design. It performs privacy impact assessments when relevant in order to ensure its standard operating procedures ensure adequate processing of personal data and that all safeguards are in place to minimize the risks identified.
EORTC performs project specific privacy impact assessment only for projects that sensibly deviate from the scope covered by standard operating procedures with regards to the purpose of processing, type of data being processed, types of activities performed, types of data recipients and/or tools and systems used.

7 DATA PROTECTION OFFICER

Given the core activities of the EORTC consist of processing on a large scale of special categories of data, including health and genetic data, EORTC appointed a Data Protection Officer (DPO) who advices EORTC and controls EORTC's compliance with applicable data protection laws and this Policy.

8 SUPERVISORY DATA PROTECTION AUTHORITY

EORTC HQ is based in Belgium. Belgian privacy commission is the EORTC's supervisory authority.

---

(1) Specific exemptions may apply for processing of pseudo-anonymous data for scientific research (for the data relative to patients and caregivers); those exemptions are applied by EORTC in accordance with GDPR and/or applicable national legislation; exemptions may also apply differently from one project to another in accordance with eventual Ethical reviews of projects.

9 RECORDS OF PROCESSING ACTIVITIES

EORTC keeps records of all processing activities it conducts as controller (alone or jointly with other controller(s)) and as processor following recommendations provided by Belgian privacy commission.

10 REFERENCES

- Universal declaration of Human rights (art 12)
- EU data protection directive 95/46/EC
- 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 Act of 8 December 1992 on the protection of privacy in relation to the processing of personal data.

11 FURTHER INFORMATION

If you have any questions regarding the provisions of this Policy, your rights under this Policy or any other data protection issues, or if you are unhappy about the way in which EORTC has used your personal data, you can contact EORTC's Data Protection Office at the address below.

Attention:	Data Protection Officer
Email:	dpo@eortc.org or privacy@eortc.org
Address:	EORTC, avenue Mounier 83, 1200 Brussels, Belgium

12 DOCUMENT HISTORY

EORTC will communicate all changes to the Policy, whether administrative or material in nature:
- to the EORTC members bound by the Policy via EORTC newsletter
- to third parties bound by the Policy, but which do not receive the newsletter, via written notice (possibly by e-mail); and
- systematically to individuals who benefit from the Policy via www.eortc.org/.

EORTC maintains an up-to-date list of the changes made to the Policy.

Version number	Brief description of change	Author	Effective date
1.0	Initial release	Anastassia Negrouk	20 Feb 2017
2.0	Update to GDPR requirements	Anastassia Negrouk	25 May 2018