CBIG-SCREEN

Working collaboratively with vulnerable women to identify the best implementation gains by screening cervical cancer more effectively in European countries

Grant Agreement No. 964049
Start date: 01. Mars 2021
Duration: 60 Months

Deliverable No 1.9
CBIG-SCREEN Data Protection Officers (DPO) and data protection policies

Nature: Report
Planned delivery date: 31. August 2021
Actual delivery date: 23. August 2021
Lead Beneficiary: Inserm, *Marc Bardou*

Dissemination level		
PU	Public	**x**
PP	Restricted to other programme participants (including Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

Table of content

1. Introduction.....3

2. List of CBIG-SCREEN Data Protection Officers (DPO) 4

3. Data Protection policies of those Beneficiaries which are not required to appoint a DPO....6

Annexes.....10

1. Introduction

European regulation 2016/679 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 - or General Data Protection Regulation (GDPR) - came into force on May 25th 2018 in all European Union (EU) Member States. Its objective is to harmonize the legal framework for data protection within the EU and uphold the European data protection model in the face of globalization, both as a factor of democracy and a competitive advantage. The GDPR is an essential step to protect fundamental rights in the digital age and is destined to ensure people trust that their data are used fairly and responsibly.

Processing of Data must comply with the following principles of protection and accountability as outlined in **Article 5.1-2** of the GPRD:

1. **Lawfulness, fairness and transparency** — Processing must be lawful, fair, and transparent to the data subject.
2. **Purpose limitation** — You must process data for the legitimate purposes specified explicitly to the data subject when you collected it.
3. **Data minimization** — You should collect and process only as much data as absolutely necessary for the purposes specified.
4. **Accuracy** — You must keep personal data accurate and up to date.
5. **Storage limitation** — You may only store personally identifying data for as long as necessary for the specified purpose.
6. **Integrity and confidentiality** — Processing must be done in such a way as to ensure appropriate security, integrity, and confidentiality (e.g. by using encryption).
7. **Accountability** — The data controller is responsible for being able to demonstrate GDPR compliance with all of these principles.

Appointed Data Protection Officers ensure, in an independent manner, that an organisation applies the laws protecting individuals' personal data. The designation, position and tasks of a DPO within an organization are described in Articles 37, 38 and 39 of the GRPD.

Organisations need to appoint a DPO if:

- they are a public authority or body (except for courts acting in their judicial capacity);
- core activities require large scale, regular and systematic monitoring of individuals (for example, online behaviour tracking); or
- core activities consist of large scale processing of special categories of data or data relating to criminal convictions and offences.

For those institutions which appointed a DPO even if not required to, the same requirements of the position and tasks apply had the appointment been mandatory.

This deliverable provides the list and contact details of the Data Protection Officers (DPO) of those CBIG-SCREEN partners with a designated DPO and a description of the Data Protection Policies of those Beneficiaries which are not required to have a DPO appointed.

2. List of CBIG-SCREEN Data Protection Officers (DPO)

The designated DPOs of the following CBIG-SCREEN Partner institutions ensure the proper execution of implemented measures to comply with GDPR requirements.

No	Participant organisation legal name	Country	Designated DPO	DPO Contact Details
1 (CO)	Institut national de la santé et de la recherche médicale - Inserm	France	Mrs Frédérique Lesaulnier	Inserm 101, rue de Tolbiac - 75013 Paris, France dpo@inserm.fr https://www.inserm.fr/en/news-and-events/news/gdpr-inserm-frederique-lesaulnier-appointed-data-protection-officer
2	Region Midtjylland - Regionshospitalet randers (RHR)	Denmark	Marie-Louise Gammelgaard Wulff	Central Denmark Region Skottenborg 26, PO Box 21, DK-8800 Viborg Tel. +45 2966 9495 dpo@rm.dk https://www.rm.dk/om-os/Dine-data/
3	London school of hygiene and tropical medicine - LSHTM	UK	Alex Hollander Head of Legal/ interim DPO	The London School of Hygiene & Tropical Medicine Keppel St, London WC1E 7HT, United Kingdom Alex.Hollander@lshtm.ac.uk https://www.lshtm.ac.uk/aboutus/organisation/data-protection
4	Azienda Unita Sanitaria Locale di Reggio Emilia - AUSL-IRCCS	Italy	Erica Molinari	Azienda Unità Sanitaria Locale – IRCCS – Reggio Emilia – Via Giovanni Amendola 2 – 42122 Reggio Emilia: Data Protection Officer - dpo@ausl.re.it Privacy Office: Head Privacy Office - privacy@ausl.re.it Web site: https://portal.ausl.re.it/Pagine/Privacy.aspx
5	Instituto de saude publica da universidade do porto - ISPUP	Portugal	Mr Vasco Dias	ISPUP Rua das Taipas, 135, Porto, Portugal dpo@ispup.up.pt

				https://ispup.up.pt/resources/downloads/Politica_de_Privacidade_ISPUP_Comunicacao_Secretaria.pdf
6	Tartu Ulikool - UTARTU	Estonia	Terje Mäesalu, Senior Specialist of Data Protection	Internal Audit Office, Ülikooli 18-244, Tartu, Estonia, andmekaitse@ut.ee https://www.ut.ee/en/data-protection-policy
7	Universitatea Babes Bolyai - UBB	Romania	Dr. Raul-Ciprian Dăncuță	Universitatea Babeș-Bolyai Str. Mihail Kogălniceanu, nr. 1, 400084, Cluj-Napoca, România dpo@ubbcluj.ro https://www.ubbcluj.ro/ro/politici/#contactGPO
8	Institute of Oncology Cluj-Napoca - IOCN	Romania	Mr. Janos GNANDT	34-35 Republicii Str., 400015, Cluj-Napoca, România janos.gnandt@iocn.ro
11	Ecole d'économie de Paris - PSE	France	Mrs Gaëlle BUJAN, CNRS Data Protection Officer	3, rue Michel-Ange - 75794 Paris cedex 16, France dpd@cnrs.fr +33 3 83 85 64 26 https://gretha.cnrs.fr/en/data-processing-and-liberties/
13	European Cancer Leagues - ECL	Belgium	Dr Wendy Yared	Association of European Cancer Leagues (ECL) Chaussée de Louvain / Leuvensesteenweg 479 Brussels ❙ 1030 ❙ Belgium wty@europeancancerleagues.org
14	Inserm Transfert SA - IT	France	Mrs Patricia Joseph-Mathieu	Inserm Transfert 7 rue Watt, 75013 Paris, France dpo@inserm-transfert.fr https://www.inserm-transfert.fr/politique-de-confidentialite-des-donnees-en/?lang=2

3. Data Protection policies of those Beneficiaries which are not required to appoint a DPO

Beneficiary P09 - European institute of women's health limited EIWH (Ireland)

The EIWH does not need to appoint a Data Protection Officer for the purpose of this project as we are not collecting or processing any large scale data, tracking individuals in any way, or have part in any large-scale systemic processing of special categories of data, nor are we a public authority or body. Nevertheless, we comply with all applicable GDPR data privacy legislation regarding the processing and storage of personal data.

We only use personal data for the purpose which the person has given their explicit permission. We provide all our users the opportunity to unsubscribe from any of our mailing lists by using an unsubscribe button that is available on our website [https://www.eurohealth.ie/privacy].

We have never and will never sell, rent, loan, trade, or lease any personal information collected by any means either online or offline. We have never used any external mail service, to reduce their ability to collect information about you and your activities. All information is kept confidential unless given explicit consent to by the user.

The EIWH have not and will not share any personal information with others. However, as can arise in our activities where we arrange cooperative actions or activities, we will endeavour to ensure that persons on our mailing list do not receive multiple invitations such co-sponsored events. In such circumstances we reserve the right to share your first name, last name, and employer with partner organisations for the sole purpose of avoiding duplications in the final invitation list. We will not share your phone number, email address, or any other contact information.

EIWH uses secure data networks that are protected by firewall and password protection systems that are consistent with industry standards. EIWH security and privacy policies are regularly and periodically reviewed and enhanced as necessary. Only authorised support staff have access to the information provided by our contacts.

Our database of contacts is located in Dublin and is placed online solely at times where information is actively being distributed. At other times the service and the information required for distribution is kept offline.

If a person wants to know what information we have about them, they have the right to ask for a copy of this information. A person has the right, at any time, of access, modification, correction and removal of their data collected in our databases.

The EIWH is the controller of personal data, under applicable data privacy legislation and in regard to the processing of personal information. For any further information, EIWH can be contacted [info@eurohealth.ie, European Institute of Women's Health, 33 Pearse Street, Dublin 2, Ireland] should anyone have any questions about our privacy practices.

Beneficiary P10 - Centre international de recherche sur le cancer – IARC (France)

IARC, as part of WHO and the United Nations System, and as per the Convention on the Privileges and Immunities of the Specialized Agencies of the UN, is not subject to EU law and regulations. Concretely, this implies that IARC/WHO is not subject to GDPR. This interpretation was recently confirmed in a response letter from the EU to the UN Office of Legal Affairs in New York. You will find enclosed this document to justify clarification about IARC's compliance with GDPR (see Annex I EC NV on GDPR).

In the meantime, all IARC European collaborators must adhere to GDPR and are unable to share personal data with IARC unless they ensure that we also apply the principles of GDPR when handling their data.

In late 2018, in order to respond to the GDPR, a large number of UN System Organisations agreed on a high-level document entitled **Personal Data Protection and Privacy Principles** (Annex II: UN PPG Draft 10 - 18 Sept 2018 FINAL). These principles aim to:

- Harmonize standards for the protection of personal data across the UN System;
- Facilitate the accountable processing of personal data for the purposes of implementing the mandates of the United Nations System Organizations; and
- Ensure respect for the human rights and fundamental freedoms of individuals, in particular the right to privacy.

In order to address the main issues arising notably due to GDPR requirements, the following steps should be considered by IARC:

- Data should be anonymized to the furthest extent possible;
- Alternatively, depending on the type of data and context, it might be preferable to ensure the data are pseudonymised;
- If necessary, it should be reasserted that IARC/IARC's collaborators shall not make any attempt to trace back the identity of individuals concerned;
- Reference may be made to the ongoing high-level discussions between the EC and UN organizations by sharing with IARC's collaborators the letter from July 2018.

IARC has not appointed a DPO, but one staff member is nominated to manage the Information Security matters.

Beneficiary P12 - Health psychology research center - HPRC (Bulgaria)

HPRC is not required to have a DPO appointed, since the beneficiary is not a public body and does not conduct large scale processing of special categories of data. HPRC follows measures that correspond to the requirements of 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 (General Data Protection Regulation), hereinafter the "GDPR".

Processing of Data complies with the following principles of protection and accountability as outlined in **Article 5.1-2** of the GPRD, namely:

1. ***Lawfulness, fairness and transparency*** — *processing and collecting data must be lawful, fair, and transparent to the data subject.* Before collecting data for research purposes, HPRC designs procedures and documents which are in concordance with legal procedures in the EU, Bulgaria and with research ethics for research subject protection. These materials are submitted for approval by the Ethics Committee of relevant professional organizations or institutions. Consent forms are prepared, which describe to the individuals the data to be collected, the rights that participants have and what the data will be used for. These are discussed with research participants, to ensure transparency; they receive a copy of the consent form and other project

materials. Signed or unsigned consent forms can be used. Participants are encouraged to ask any clarifying questions. Other data for our organizational contacts are also collected through explanation of the purpose for collecting it (for example - information about event, partnership in projects, participation in projects, invitations to events, etc.)

2. ***Purpose limitation*** *— Personal data are only collected for specific, explicit and legitimate purposes and may not be further processed in a way incompatible with those purposes*. The purpose for which data are collected are described openly to participants, through discussion of the aims and goals of the project or other reason for data collection. These are also included in the submission to the Ethics Committees. The data cannot be used or analysed for other purposes.

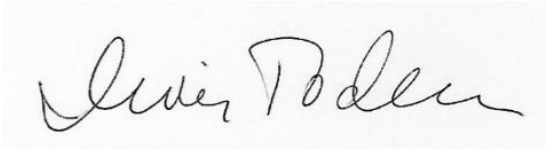
3. ***Data minimization*** *— only personal data, which is relevant and limited to what is necessary for the purposes for which they are processed*. Generally identifying data is not collected by HPRC for research purposes, and thus the data collected are limited to broad demographic characteristics (age, ethnicity, gender, in some cases city of residence). In the rare cases that identifiable personal data are collected (such as names and contact information for follow-up interviews), that is done only if the participants voluntarily submit that information and is later de-identified when no-longer needed for contact.

4. ***Accuracy*** *— Personal data must be accurate and, if necessary, kept up to date; all reasonable measures must be taken to ensure the timely deletion or correction of inaccurate personal data, taking into account the purposes for which they are processed*. Generally identifying data is not collected by HPRC. In the rare cases that identifiable personal data are collected, we would ask the participants to contact us to update changed data if necessary. We would delete any additional data that are collected but are not relevant to the purpose of the project.

5. ***Storage limitation*** *— the personally identifying data is kept for as long as necessary for the specified purpose*. In designing research projects, we specify the length of time for which the data will be stored (and submit that information also to the Ethics committee). Electronic data are stored only on designated computers and paper data are stored only in designed locked spaces in the office of HPRC. After the term for storage has expired, we delete the data from all computers through permanent deletion; and all paper files are deleted through shredding.

6. ***Integrity and confidentiality*** *— Processing must be done in such a way as to ensure appropriate security, integrity, and confidentiality.* The data are stored in a secure location such as designated for the purpose locked cabinets and/or password protected computers. Computers are additionally protected through firewall, anti-virus software, malware and ransomware protection. Identifiable data are given a de-identified code and the table with a correspondence of the code to the personal name (if it is necessary to store that information) is kept in a locked cabinet. This ensures anonymity of participants, who are informed of these procedures before the initiation of the projects. They are also informed that they can leave the project before and during the data collection (and delete their data), and in some cases after the data have been processed, if it can be identified to be theirs). Access to identifiable personal data is limited to the Director of HPRC and only to specific HPRC staff, who are named in Ethics protocols. All other staff have access only to the de-identified data. No one in HPRC distributes personal data collected for research purposes to other contacts.

7. **Accountability** — Accountability is ensured through periodic training of staff and research team members. Regular team meetings are held for discussion of data status, storage, accuracy, necessity and purposes for which they are used, as well as compliance with the Ethics protocols. Accountability is also ensured through periodic resubmission and reporting to the Ethics Committees.



Irina Todorova, Director of HPRC

Annexes