CropBooster-P

Deliverable 7.2 (POPD - Requirement No. 2)

Title: Ethics requirements for studies involving human participants in CropBooster-P

Start date of the project: **November 1st, 2018** / Duration: 36 **months**

Planned delivery date: M1 (November 2018)

Actual submission date: 21 November 2018

Work package: WP7 / Task: 7.1 & 7.2

Work package leader: WUR

Deliverable leader: WUR

Version: 1

Date of version: November 2018

Dissemination level	
~~Public~~	
~~Classified, as referred to Commission Decision **2001/844/EC**~~	
Confidential, only for members of the consortium (including the Commission Services)	*X*

Table of Contents

Data protection by partners

Cropbooster-P partners with access to any of the personal data on human being collected or analysed within the Cropbooster-P project should either

- have a predetermined data protection protocol overseen by a data protection officer,. Contact data of the data protection officer must be provided in this document, and must be kept up to date.
- create a detailed data protection plan. This plan must be completed prior to gaining access to personal data on human beings and must be submitted to Cropbooster-P as appedix to D7.2 and kept on file.

Partners with an appointed Data protection officer

CropBooster-P partners involved with collection and or analysis of participant data with an appointed Data Protection Officer (DPO). The contact details of the DPO of the task-leader (or the partner responsible for secure storage of the data) are made available to data subjects involved in the research.

If a DPO of a beneficiary changes the beneficiary will inform CropBooster-P management, after which this deliverable will be updated.

List of DPO-officers CropBooster-P partners as of November 2018.

WR	yes	Frans Pingen functionarisgegevensbescherming@wur.nl
VIB	yes	through a joint-venture agreement have access to the university DPO structures for research activities involving sensitive human personal data.
WU	yes	Frans Pingen functionarisgegevensbescherming@wur.nl
CNR	yes	Giuliano Salberini
EPSO	no	
UDUS	yes	Kurt Finkbeiner Building: 25.13 Floor/Room: 00.34 Phone +49 211 81-13214 Datenschutzbeauftragter@hhu.de
UNOT	yes	Data Protection Officer, Legal services A5, Trent Building, University of Nottingham, University Park, Nottingham Ng7 2RD dpo@nottingham.ac.uk.
JKI	yes	Andreas Willems, head of legal office andreas.willems@julius-kuehn.de
CNRS	yes	Gaëlle Bujan, dpd.demandes@cnrs.fr
UCPH	yes	Lisa Ibenfeldt Schultz Telephone+45 29 61 16 67 Email dpo@adm.ku.dk
INRA	yes	Nathalie GANDON nathalie.gandon@inra.fr Tèl. : +33 1 (0)5 61 28 54 37 Port : +33 1 (0)6 68 41 64 54 24, Chemin de Borde Rouge - Auzeville - CS 52627 31326 Castanet Tolosan Cedex France https://intranet.inra.fr/cil-dpo
ETP	No	
ULANC	yes	Mike Abbotts, Information Governance Manager Email: michael.abbotts@lancaster.ac.uk Phone: 01524 510841
USAMV	yes	Mircea Grigoras magrigoras@yahoo.com
ESA	no	
ACTA	no	

Partners without an appointed Data protection officer

Beneficiaries not required to appoint a DPO under the General Data Protection Regulation 2016/679 (GDPR), will either have no access to data from participants or create a detailed data protection policy which will be submitted as deliverable and kept on file and be provided to the agency for review on request.

This data protection policy should conform with https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_en.htm

Details of the plan may be informed with information from http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-data-protection_en.pdf It should however be noted that this document has no official status.

For partners that do not have a DPO this means they should create a data protection plan in which they identify:

1) how protection of personal data is safeguarded to prevent unauthorised access
2) how records are kept
3) how data breaches will be handled
4) personal data is not shared outside the EU
5) how data minimisation principles are safeguarded by justifying the need for collecting and analysing the specified data
6) How anonymization and/or pseudonymisation are conducted
7) how consent is obtained in line with rights and freedoms of research participants
8) within the given consent, that such consent is gained and stored,
9) a procedure is in place where participants can gain a copy of, can review and correct, or achieve erasure of personal data
10) that contact information about the partner is transparent and accessible to participants
11) how response to participant requests are handled
12) In case sensitive data is used, justification for their collection is givens
13) In case re-analysis of existing data is conducted how the partner ensures legal ground to access that data.