Value and Impact through Synergy, Interaction and coOperation of Networks of AI Excellence Centres

GRANT AGREEMENT NUMBER: 952070

Deliverable D7.2

Processing of Personal Data

POPD - Requirement No.2

Project title	**VISION - Value and Impact through Synergy, Interaction and coOperation of Networks of AI Excellence Centres**
Grant Agreement number	952070
Funding scheme	Horizon 2020
Start date of the project and duration	1 September 2020, 36 months
Project coordinator name	ULEI - UNIVERSITEIT LEIDEN – Holger Hoos
Deliverable number	D7.2
Title of the deliverable	POPD - Requirement No.2
WP contributing to the deliverable	WP7 – Ethics requirements
Deliverable type	R - Report
Dissemination level	Confidential, only for members of the consortium (including the Commission Services)
Due submission date	31 October 2020
Actual submission date	June 2021
Partner(s)/Author(s)	Wendy Aartsen (ULEI)
Internal reviewers	Phillip Slusallek – Director Ethics Vit Dočkal – technical compliance Giovanna Galasso, Costanza Bersani – formal review

Disclaimer

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 952070. This document has been prepared for the European Commission, however, it reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein

History of changes		
When	**Who**	**Comments**
28 January 2021	Wendy Aartsen	Version 1.0
15 May 2021	Ricardo Catalan	Final internal review Leiden University
28 May 2021	Costanza	Review
05 June 2021	Wendy Aartsen	Submission Executive Board for approval

Confidentiality	
Does this report contain **confidential** information?	Yes X No ☐
Is the report **restricted** to a specific group?	Yes X No ☐ *If yes, please precise the list of authorised recipients*: Consortium members and EC

Table of Contents

Executive summary

The purpose of this Deliverable 7.2 is to provides detailed information on the procedures that will be implemented for data collection, storage, protection, retention and destruction. It includes the scope and extent of the data used and all measures taken to ensure the protection of personal data required under the GDPR. The document describes the measure and procedures to be followed compliant to the GDPR implementations at Leiden University; coordinator for the VISION project. The content of the document has been reviewed and approved by the Data Protection Officer of the Leiden University.

1 Introduction

The European Commission has identified different ethics issues that may arise during research projects, together with specific requirements that projects shall satisfy for each of these issues. This deliverable regards the ethical issues concerning any research involving the processing of personal data (POPD).

1.1 Purpose and structure of the document

The deliverable describes how VISION addresses and manages the ethical implications following processing of personal data. Specific attention will be given to:

1. The beneficiary must confirm that it has appointed a Data Protection Officer (DPO) and the contact details of the DPO are made available to all data subjects involved in the research. For host institutions not required to appoint a DPO under the GDPR a detailed data protection policy for the project must be included in the ethics deliverable.
2. The beneficiary must explain how all of the data they intend to process is relevant and limited to the purposes of the research project (in accordance with the 'data minimisation 'principle). This must be included in the ethics deliverable.
3. A description of the technical and organisational measures that will be implemented to safeguard the rights and freedoms of the data subjects/research participants must be included in the ethics deliverable.
4. A description of the security measures that will be implemented to prevent unauthorised access to personal data or the equipment used for processing must be included in the ethics deliverable.
5. A description, if applicable, of the anonymisation/pseudonymisation techniques that will be implemented must be included in the ethics deliverable.
6. In case personal data are transferred from the EU to a non-EU country or international organisation, confirmation that such transfers are in accordance with Chapter V of the General Data Protection Regulation 2016/679, must be included in the ethics deliverable.
7. In case personal data are transferred from a non-EU country to the EU (or another third state), confirmation that such transfers comply with the laws of the country in which the data was collected must be included in the ethics deliverable.
8. Templates of the informed consent forms and information sheets relevant to the storage and processing of personal data must be kept on file (to be confirmed in the ethics deliverable).
9. In case the research involves profiling, the beneficiary must provide explanation how the data subjects will be informed of the existence of the profiling, its possible consequences and how their fundamental rights will be safeguarded. This must be included in the ethics deliverable.

10. An explicit confirmation, where relevant, that the data used in the project is publicly available and can be freely used for the purposes of the project must be included in the ethics deliverable.
11. In case of further processing of previously collected personal data, an explicit confirmation that the beneficiary has lawful basis for the data processing and that the appropriate technical and organisational measures are in place to safeguard the rights of the data subjects, must be included in the ethics deliverable.

2 Data protection and privacy

Specific security and privacy issues at system level will be treated in individual tasks. The platforms, tools and algorithms used for processing any personal data in the project will be selected to ensure privacy and confidentiality. To the extent that we will use the platform provided by the AI4EU project, we will assume that privacy and confidentially requirements have been ascertained by AI4EU.

The partners agree that any Background, Results, Confidential Information and/or any and all data and/or information that is provided, disclosed or otherwise made available between the partners of the consortium during the implementation of the project and/or for any exploitation activities ("Shared Information"), shall not include personal data as defined by Article 4, Chapter 1 of the General Data Protection Regulation (EU 2016/679) (hereinafter referred to as "Personal Data").

Accordingly, each partners of this consortium agrees that it will take all necessary steps to ensure that all Personal Data is removed from the Shared Information, made illegible, or otherwise made inaccessible (i.e., de-identified) to the other partners prior to providing the Shared Information to such other partners. Each partner who provides or otherwise makes available to any other partner Shared Information represents that:

(i) it has the authority to disclose the Shared Information, if any, which it provides to the partners under the project's Consortium Agreement;

(ii) where legally required and relevant, it has obtained appropriate informed consents from all the individuals involved, or from any other applicable institution, all in compliance with applicable regulations; and

(iii) there is no restriction in place that would prevent any such other partner from using the Shared Information for the purpose of this project and the exploitation thereof.

2.1 Personal data

For the purpose of this project, it might occur that the collection and use of personal data/information of human individuals is needed. A privacy policy has been adopted at ULEI consisting all major GDPR principle including but not limited to data minimization will be adopted to ensure that only data that are strictly necessary for running the project will be processed (see annex 1). VISION does not intend to apply automated decision making or profiling. All processing activities will be documented, in compliance with the accountability requirements of the GDPR.

2.2 Data collection and processing

In VISION, by default, all data will be at least pseudonymised. For any data that identifies an individual, by name or other identifying feature, that individual must give informed consent to its use in advance.

Confidentiality will be maintained in a manner commensurate with the needs of the project. When the information sought is sensitive (so that the effect of any disclosure would be negative and significant to individuals) the provision of confidentiality is essential to protect the individuals. Therefore, we will follow disciplinary best practices and engage any common law or statute-based legal protections that are available to maximize protection of individuals. Related data-sets generated in VISION will be catalogued and stored centrally using cloud storage and backup solid state storage, data management system (DSM).

2.3 Data security

Special attention will be given to the confidentiality and implement all appropriate technical and organizational measures necessary to protect potential personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and against all other unlawful forms of processing, taking into account the particularity of the performed processing operations. Only authorised user will be granted access for data handling, access for information or data input (even change). Non-sensitive data (including publications, source codes, etc.) will be made open access wherever possible (e.g. Green and Gold routes to open access publishing). Staff involved will be required to sign a confidentiality statement. After collection, data will be coded at the local level, electronically encrypted and shared for study purpose only in aggregated form within the DSM.

Appropriate measures will be taken to prevent unauthorized use of any individual's information. ULEI has a dedicated University Data Protection Officer:

Ricardo Catalan r.m.catalan@bb.leidenuniv.nl

Institutional procedures are in place to obtain approval of personal data in accordance with institutional policy and national law. They will adhere to the provisions set out in the:

- Directive 2006/24/EC of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communication services or of public communications networks.
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)
- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

2.4 Data management plan

A Data Management Plan (DMP deliverable D2.3) will be developed to be applied throughout the project with regard to all the datasets that will be stored and used. The DMP will be a living document updated during the course of the project. With the aim to foster a stream-lined discussion on AI ethics and to enable uniform application of its principles across the NoEs, VISION will install an Ethics Board, and the DMP will contain the generic procedure defined to facilitate the ethics approval procedure for all NoEs networks, to ensure a smooth and uniform process aligned between all networks. The DMP

will be aligned where possible to the FAIR principles of data management promoting mechanisms for finding the right data, making it accessible to interested parties, as well as advancing interoperability and reusability. As part of the DMP, the Data Protection Impact Assessment (DPIA) has already been completed and reviewed by the Data Protection Officer, see section 3.

2.5 Ethics board

As part of its coordination and support mandate, VISION will install an Ethics Board composed of ten members, two representatives per NoE consortium and two representatives from VISION. VISION will provide the administrative support to the Ethics Board in designing and running a common process for ethics advice and approval. This will ensure that the approach of all four networks will be aligned with each other, with the European Union's vision and with current AI ethical and legal discussions, while at the same time profit from the extensive experience from leading international AI ethics experts from within the four NoE networks, such as Virginia Dignum, Jeroen van den Hoven and Barry O'Sullivan. Drafting ethics guidelines and recommendations for broader AI policy is in the hands of the high-level expert group on AI with support of the European AI Alliance. The aligned process towards ethical approval defined by the VISION ethical board will adhere to the white paper" A European approach to excellence and trust", the COM (2019) Building Trust in Human-Centric Artificial Intelligence and its 7 key requirements for trustworthy AI.

2.6 Misuse

VISION will follow the European Code of Conduct for Research Integrity in dealing with scientific misconduct. As part of the institutional Human Resource (HR) matters, all beneficiaries have procedures for reporting, investigating and dealing with misconduct and fraud. The consortium will adhere to local university/institute HR rules in the event of an allegation of misconduct or fraud, particularly as to fairness and thoroughness of investigation and confidentiality. The VISION consortium will adhere to local university/institute HR rules in the event of an allegation of misconduct or fraud, particularly as to fairness and thoroughness of investigation and confidentiality. In case of fabrication, falsification and plagiarism, the coordinator or the Ethics Advisor within the Executive Board (in case of misconduct by the coordinator), will report to the Steering committee and notify the responsible institution to start local procedures. The HR department will take all necessary corrective actions if the allegation is founded, and the Project Officer will be notified.

Potential corrective actions may include, but not limited to:

- Retraction/correction of articles in journals or other published material;
- Withdrawal/repayment of funding;
- Notification of other employing institutions;
- Notification of other organisations involved in the research, including the funders of the research;
- Release of any public statements necessary to protect the good name and reputation of the participating institutions

3 Data Protection Impact Assessment (DPIA)

POPD – Requirement No.2

Universiteit Leiden

Instructions:
For each personal data process, fill out which data is being used. *If there is not enough space, you may add rows to this sheet*. Don't worry about whether the sheet will be messy.
Each phase of the research is a separate process, unless they use the data in the same way and rely on the same processing ground.
Explanations of the fields can be read by moving the mouse over the field. Here it will also be mentioned if the fields should always be filled, or whether they are not always applicable.
In case of questions, ask your information manager or the Data Protection Officer.

Research Data Processing Inventory

Title of your research:	Researcher(s):	Research number (if applicable):
VISION	Holger Hoos	952070

Categories of processing (11):

personal identification personnel

Involved responsible parties (12):	Country (13):	Internal/External (14):
Leiden University	Netherlands	Internal
Czech Technical University	Czech Republic	External
German Research Center for Artificial Intelligence	Germany	External
University College Cork	Ireland	External
Fondazione Bruno Kessler	Italy	External
Institut National de Recherche en Informatique et Automatique	France	External
Nederlandse Organisatie voor toegepast-natuurwetenschappelijk Onderzoek	Netherlands	External
PricewaterhouseCoopers Advisory	Italy	External
THALES SIX GTS France	France	External

Processor(s) (15):	Country (16):
Hands4Grants B.V.	Netherlands
Data storage provider	
Mattermost	France

Categories of data subjects (persons involved) (17):

personnel and project members

Faculties & department (18):	Country (19):	Internal/External (20):
Leiden University LIACS	Netherlands	Internal
Czech Technical University	Czech Republic	External
University College Cork	Ireland	External

Recipients (21):	Country (22):	Internal/External (23):

Personal data collected (24):	Classification (25):	Source (26):	Processing purpose (27):	Processing ground (28):	Contact person (29):	Storage period (30):	Justification of storage period (31):	International Transfer? (32)	Storage (33):
names and email adresses	normal	him/herself	communication	1. Consent has been obta	Holger Hoos	7 years	Communication during the project	EU based secured cloudstorage	cloudstorage
communication	Normal	him/herself	communication	5. Processing is necessary	Holger Hoos	7 years	Communication during the project	EU based secured cloudstorage	cloudstorage

Has consent been obtained for the sensitive personal data? Please explain, if applicable (34):

No, public interest

Are you re-using personal data from previous research? If so, please explain (35):

No.

Can the use (or misuse) of the personal data in your research lead to limitations of data subjects' rights? If so, please explain (36):

Yes, in case the data storage is unsecure or misuse by recording meeting audio.

Are there any laws (besides the GDPR) applicable to the processing of personal data during your research? If so, please explain (37):

No.

Universiteit Leiden

Description of Risks and Corrective Measures

Processes research	Select type of personal data involved:	Risks (after corrective measures are taken)	Likelihood	Impact	Corrective measures (this does not contain the measures that are always necessary, such as a privacy notice before collection from data subject)
E-mail correspondence	Only normal personal data	E-mails leak, and personal data of data subjects becomes public, resulting in (a.o. reputational) damage to the data subjects	1	2	Use University e-mail
Survey via external supplier (e.g. Qualtrics)	Not applicable - no personal data	#N/A	#N/A	#N/A	#N/A
Storage of and access to digital research data (at the University)	Only normal personal data	Stored data is accessed unauthorized, and data of research becomes public, resulting in damage to the research	1	2	Store the information in a way shielded from others. Either encrypted, or on a storage medium only accessible for the researchers
Storage of and access to digital research data (from home or other non-University location)	Only normal personal data	Stored data is accessed unauthorized, and data of research becomes public, resulting in damage to the research	1	2	Same as from University, with the added requirement of connecting through VPN and a daily scan with an up-to-date virus and malware scanner
Physical storage of research data (e.g. documents, biological samples, etc.)	Only normal personal data	Stored data is accessed unauthorized, and data of research becomes public,	1	2	Store the data behind lock and key
Recording images/videos	Not applicable - no personal data	#N/A	#N/A	#N/A	#N/A
Transfer of data externally in the context of a collaboration/partnership	Only normal personal data	Transferred data is accessed unauthorized, and personal data becomes public	1	2	Ensure there is a collaboration agreement with the required personal data clauses
Transfer of data externally for research support (e.g. as a scholarship condition)	Only normal personal data	Transferred data is accessed unauthorized, and personal data becomes public	1	2	Ensure it is absolutely required to send the data. If possible, send the data anonymized (probably not possible, but then go for pseudonimized).
Combining data sets from previous research	Not applicable - no personal data	#N/A	#N/A	#N/A	#N/A
Data subject GPS tracking, or using data from wearables	Not applicable - no personal data	#N/A	#N/A	#N/A	#N/A
Re-use of personal data for long lasting research	Not applicable - no personal data	#N/A	#N/A	#N/A	#N/A
Requesting/receiving personal data from external agencies	Only normal personal data	Receiving more information that needed for the research, resulting in processing (storing) personal data without a valid processing ground	1	1	During the data request, ensure not more data than needed is requested
Pre-screening potential data subjects (targeted)	Not applicable - no personal data	#N/A	#N/A	#N/A	#N/A
Pre-screening potential data subjects (untargeted)	Not applicable - no personal data	#N/A	#N/A	#N/A	#N/A
Using external employees/students to assist during the research	Only normal personal data	External employees leaking data, followed by unauthorized access	1	2	Allow students/employees to only work at the University and instruct them not to copy the data.
Use of external suppliers of services (e.g. storage or analysis)	Only normal personal data	External services leaking data, followed by unauthorized access	1	2	Require a processor agreement
Usage of researchers personal e-mail	Only normal personal data	Loss of control over the personal data, followed by unauthorized access	1	2	The use of personal e-mail addresses is not allowed. Only use University e-mail addresses.
Monitoring of data subjects (e.g. via video, data use analysis, online activity, etc.)	Not applicable - no personal data	#N/A	#N/A	#N/A	#N/A
Logging of data from data subjects	Not applicable - no personal data	#N/A	#N/A	#N/A	#N/A
Deleting research data (par of the data, or all of the data)	Not applicable - no personal data	#N/A	#N/A	#N/A	#N/A

4 Annexes

Annex 1 data minimization policy is part of the Information Security Guidelines

Executive summary of the official guidelines to the Information Security at the Leiden University.

Information security is a hot topic. Every day the media report on subjects topics such as botnets, the interception of information by (foreign) governments, DDOS attacks on banks, viruses that cause money to be withdrawn from accounts, spam and phishing and other malware.

This makes it clear that more attention needs to be paid to these issues and that the attention should be paid to these matters and that measures should be taken to repel these attacks.

As a result of the above developments, the Dutch cabinet has therefore seen fit to establish a National Cyber Security Centre (NCSC). Its task is to increase the resilience of Dutch society in the digital domain by advising on how to make systems more secure. Institutions such as Leiden University are expected to take this advice on board in their own policy.

Information security at Leiden University is not just a supporting process. Knowledge institutes also play a role in the research into developments in the field of computers and software. Think, for example, of LIACS, where research is focused on algorithms for information security and the International Centre for Counter-Terrorism (ICCT) where cyber-security is one of the focal points.

Leiden University, like many other organizations, is increasingly dependent on information stored in (mostly automated) systems. This dependence creates new vulnerabilities and risks that need to be mitigated with appropriate measures. Insufficient information security can lead to unacceptable risks in the execution of education and research and in the research and the business operations of the university. Incidents and breaches in these processes can lead to financial and image damage.

The Executive Board (CvB) therefore wants to systematically pay attention to the security of the information systems. The previous information security policy and the baseline (minimum measures) derived from it dates from 2010 and are in need of revision. Revision is desirable because there are always new trends and developments that influence information security. The governance model has also been expanded and the policy relating to business continuity has been added.

The policy and baseline of minimum measures were drawn up under the responsibility of the Information Management Department of the Executive Office, in close consultation with the information managers of the faculties, the security officer of the ISSC and the security manager of Real Estate. This policy with respect to information security is one of the four priorities in the ICT infrastructure and ICT services as expressed in the ICT multi-year plan 2012-2015. Full document is available online:

https://www.medewerkers.universiteitleiden.nl/binaries/content/assets/ul2staff/reglementen/ict/informatiebeveiliging.pdf