

2024-04-29 FaradAI 3.1 Ethical Questionnaire/Signed Declaration - RTU

Objective: Riga Technical University (RTU)'s proposal to incorporate a new internal dataset comprising aerial drone video footage of military vehicles from the conflict in Ukraine in support of FaRADAI research activities

Preliminary discussions between CERTH, Riga Technical University (RTU), C&V Consulting highlighted the necessity of assessing its feasibility within the project's ethical and legal framework, and it was agreed to initiate the following questionnaire to answer the main concerns in this regard.

Recognising the potential value of this dataset for training purposes in WP6 and beyond and seeking confirmation regarding its ethical and legal permissibility within the project, the main concerns for C&V Consulting encompass a multifaceted array of ethical and legal considerations crucial to the integrity and compliance of the project.

Foremost among these concerns is data protection legal compliance, ensuring that the collection, processing, and sharing of data adhere to the stringent standards and provisions set forth by the European Union in the EU Charter of Fundamental Rights and the Treaty on the Functioning of the European Union (Articles 8, 9, 89), and the EU's 2016 General Data Protection Regulation (Articles 4, 5, 7, 22, 32, 35).

In addition, C&V Consulting places particular emphasis on assessing the reliability of all data, in order to avoid damaging consequences in terms of compliance with ethical rules in the event of operational use of unreliable data.

Purpose and scope of the questionnaire

- Clarify the essential purpose of the data collection, highlighting how it fits in with the overall objectives of the project.
- Explain how this process makes a significant contribution to the project.
- Enable the Ethics Advisory Board to identify potential risks and develop appropriate mitigating plans.

Questionnaire:

Data collection

Describe the data collection methodology in detail:

1. Who is in charge of the processed data and who decides how these data will be used? Who determines the purposes and the means of the processing operation(s)? Please indicate full contact details.

Riga Technical University (RTU) is in charge of the processed data and will decide how these data will be used. The purposes and the means of the processing operation(s) will be determined by the RTU. The contact details are as follows: Dr. Evalds Urtans, Lead Researcher, Riga Technical University, e-mail: evalds.urtans@rtu.lv, Phone: +31726401317. RTU will abide by the ethical and legal standards set forth by the European Union in the EU Charter of Fundamental Rights and the Treaty on the Functioning of the European Union (Articles 8, 9, 89), and the EU's 2016 General Data Protection Regulation (Articles 4, 5, 7, 22, 32, 35).

2. Identify in detail the types of data that will be collected, emphasising the relevance and legitimacy of each category to the activity. Identify the volume of data that will be gathered, emphasizing the exact volume of data needed in order to achieve the purpose of this activity (data minimisation).

The data collected will consist of aerial drone video footage of military vehicles from the conflict in Ukraine only from publicly available sources. The volume of data that will be gathered will be the minimum necessary to achieve the purpose of segmenting and classifying military vehicles. Usually, the volume of data needed to achieve this purpose is around 1000-10000 images per class. Classes will include tanks, armoured personnel carriers, self-propelled artillery, and other military vehicles. The lawful basis of personal dataprocessing is the legitimate interests of the data controller according to art. 6(1) (f) GDPR. Data will be processed only for scientific research purposes.

3. Can you achieve the same purpose without processing, by processing less data or by processing in another more obvious or less intrusive way?

No, the purpose of segmenting and classifying military vehicles from aerial drone video footage of the conflict in Ukraine cannot be achieved without processing the data. Synthetic data generation is not an option, as it is not possible to generate realistic synthetic data for this purpose. Synthetic data generation is not yet at a level where it can be used for training deep learning models for segmenting and classifying military vehicles from aerial drone video footage. Moreover, even to train synthetic data generation models,

real data is needed. Choice of Ukraine conflict data is due to the availability of the data and the fact that it is not possible to generate realistic synthetic data for this purpose. No other military conflict have such a large amount of publicly available data as the conflict in Ukraine.

4. What specific objectives does the data collection and processing serve within the broader goals of the project?

The specific objectives of the data collection and processing are to segment and classify military vehicles from aerial drone video footage of the conflict in Ukraine. This will serve the broader goals of the project by providing a new internal dataset for training purposes in WP6 and beyond. Data can be used also to train image generation models and other models in the future. This dataset would also be significant addition to validate if models trained on synthetic data would work on real data.

5. Could you elaborate on why the project's aims cannot be fully realised without the type of data being collected and processed?

Without this dataset FaradAI would not be able to validate the models trained on synthetic data. It would also add significant value to demonstrate stakeholders the potential of the models in real-world scenarios.

6. Does this action involve handling personal data on a significant scale, or systematically monitoring a publicly accessible area on a large scale?

No, this action does not involve handling personal data on a significant scale, or systematically monitoring a publicly accessible area on a large scale. The data collected will consist of aerial drone video footage of military vehicles from the conflict in Ukraine. The data will not intentionally contain any personal data.

7. Do sensitive data processing techniques apply to the project? (e.g. covert observation, surveillance, tracking or deception of individuals, camera systems to monitor behaviour or record sensitive information, data mining including data collected from social media networks, behavioural profiling of individuals and groups, use of artificial intelligence to analyse personal data...)

No, sensitive data processing techniques do not apply to the project. The data collected will consist of aerial drone video footage of military vehicles from the conflict in Ukraine. The data will not intentionally contain any personal data. Data will not contain sources of sensitive data such as social media networks, behavioral profiling of individuals and groups, or any other sensitive data sources.

8. Which communication channels will be used to collect data?

The communication channels will include open Telegram groups and open X (former Twitter) accounts. All collected data will be from open sources. Telegram and X's EULA will be followed.

9. Some channels may be encrypted (e.g. Telegram groups), but are you going to access to them? How will it be accessed? Are you going to use the Telegram API? How will user privacy be guaranteed?

Yes, Telegram and Twitter API will be used to access the data. User privacy will be guaranteed by following the Telegram and X's EULA.

10. If applicable, explain the verification protocols that will be put in place to guarantee access control, authenticity and traceability of all data collected.

Data access control will be implemented according to FaradAI's data access control policy. Data would be stored on the RTU servers and would be accessible only to the researchers involved in the project using authentication procedure. Authenticity and traceability will be manually verified by the researchers involved in the project.

11. Do you envisage any mitigation measures to ensure that videos do not identify prisoners of war in accordance with the Law of Armed Conflict and International Humanitarian Law? (e.g. Article 13 Geneva Convention III, 1949; Article 75 Additional Protocol, 1977)

Yes, automatic detection of people in the videos will be implemented. Parts of the videos that contain people will be scrambled or removed. Human researchers will also manually verify the videos to ensure that they do not identify prisoners of war in accordance with the Law of Armed Conflict and International Humanitarian Law.

12. Will measures be taken to detect and either exclude videos that identify human beings or minimise the risk of facial recognition (e.g., anonymisation, pseudonymisation, data minimisation)? If yes, which? How do they work?

Yes, measures will be taken to detect and either exclude videos that identify human beings or minimise the risk of facial recognition. Automatic detection of people in the videos will be implemented. Parts of the videos that contain people will be scrambled or removed. Human researchers will manually selectively verify results of automatic detection of people in the videos to ensure that they do not identify human beings.

13. How reliable are these techniques?

Accuracy of Human detection models to detect if person is present at all in the video frame is around 87.07% (<https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10081816/>).

14. Will the teams involved in validating the data be specifically trained to detect faked videos?

Yes, the teams involved in validating the data will be specifically trained to detect faked videos. They will be trained to detect faked videos by using state-of-the-art deep learning models for detecting faked videos and by using manual verification.

15. If applicable, how will the data subjects be informed about the processing and how can they exercise their rights as those envisioned in GDPR?

The data subjects will be informed about the processing by following the Telegram and Twitter EULA. Data will not be made public outside the FaradAI project. Data subjects will not be able to exercise their rights as those envisioned in GDPR, as the data will not intentionally contain any personal data. In case of unintentional collection of personal data, we need to notify the data subjects of this activity based on Article 14 of GDPR.

Data storage and distribution

1. What security, technical and organisational measures do you implement in order to ensure data security and integrity?

Data will be stored on the RTU servers and will be accessible only to the researchers involved in the project using proper authentication and verification procedures. Data will be stored on the RTU servers for the duration of the project. Data will be encrypted and anonymized. Access rights will be managed by the researchers involved in the project. Procedures for dealing with data breaches and notification of breaches to the national supervisory authority or to the affected individuals will be adopted.

2. On which platform will the data be stored? For how long?

Data will be stored on the RTU servers for the duration of the project.

3. What protocols will be put in place to guarantee the proper protection of the data stored on the platform?

Data will be encrypted and anonymized. Access rights will be managed by the researchers involved in the project using proper authentication and verification procedures. Procedures for dealing with data breaches and notification of breaches to the national supervisory authority or to the affected individuals will be adopted.

4. Will the data and/or the devices on which they are stored be encrypted/anonymised? How?

It will be stored in password protected format which is encrypted.

5. Describe the type of audience to which the data will be made accessible once it has been collected.

The data will be made accessible to the researchers involved in the FaradAI project only, on a need-to-know basis. The data will not be made public outside the FaradAI project.

6. Will access rights be managed? If so, do you consider appointing a manager?

Yes, access rights will be managed by RTU and appointed manager will be Dr. Evalds Urtans, Lead Researcher, Riga Technical University. If needed, access rights can be managed by other appointed managers from FaradAI project

7. What precautions will be taken by RTU in the event of the rest of the relevant partners downloading data?

The data will be stored on the RTU servers and will be accessible only to the researchers involved in the project using proper authentication and verification procedures. Data will be stored on the RTU servers for the duration of the project. Data will be encrypted and anonymized. Access rights will be managed by the RTU and FaradAI FDR managers.

8. Have you adopted or will you adopt procedures for dealing with data breaches and notification of breaches to the national supervisory authority or to the affected individuals, if applicable?

All data breaches will be reported to the national supervisory authority or to the affected individuals. Procedures for dealing with data breaches and notification of breaches to the national supervisory authority or to the affected individuals will be adopted.

The undersigned organization, Riga Technical University (RTU), through the signature of its authorized representative below, solemnly declares the veracity of all responses provided herein and the commitment to all applicable national and European legislations.

For RTU,

Signature:



Date: 22.05.2024

Place: Riga

Name: ĒVALDS URTANS

Title: DR.