FWO DMP Template - Flemish Standard Data Management Plan

Project supervisors (from application round 2018 onwards) and fellows (from application round 2020 onwards) will, upon being awarded their project or fellowship, be invited to develop their answers to the data management related questions into a DMP. The FWO expects a **completed DMP no later than 6 months after the official start date** of the project or fellowship. The DMP should not be submitted to FWO but to the research co-ordination office of the host institute; FWO may request the DMP in a random check.

At the end of the project, the **final version of the DMP** has to be added to the final report of the project; this should be submitted to FWO by the supervisor-spokesperson through FWO's e-portal. This DMP may of course have been updated since its first version. The DMP is an element in the final evaluation of the project by the relevant expert panel. Both the DMP submitted within the first 6 months after the start date and the final DMP may use this template.

The DMP template used by the Research Foundation Flanders (FWO) corresponds with the Flemish Standard Data Management Plan. This Flemish Standard DMP was developed by the Flemish Research Data Network (FRDN) Task Force DMP which comprises representatives of all Flemish funders and research institutions. This is a standardized DMP template based on the previous FWO template that contains the core requirements for data management planning. To increase understanding and facilitate completion of the DMP, a standardized **glossary** of definitions and abbreviations is available via the following link.

1. General Project Information	
Name Grant Holder & ORCID	Donatella Van Biervliet 0000-0002-8055-5641
Contributor name(s) (+ ORCID) & roles	Prof. Dr. Jeroen Maesschalck (0000-0002-0814-6835) - supervisor
Project number[1] & title	11B5723N Rebooting protest policing? Understanding technology-informed protest management practices by command post operators
Funder(s) GrantID[2]	NA
Affiliation(s)	x KU Leuven ☐ Universiteit Antwerpen ☐ Universiteit Gent ☐ Universiteit Hasselt ☐ Vrije Universiteit Brussel ☐ Other: Provide ROR[3] identifier when possible:
Please provide a short project description	The use of internet sources by protesters has several implications for public order policing, as mobilisations scale up more quickly and the crowds are more likely to take the form of non-hierarchical structures and unstable relations (Tarafdar & Ray, 2021). Partly in response to these changes, the police have adopted technologies to try and 'reboot' their public order policing: CCTV, body-worn cameras, drones, facial recognition technology, automatic number plate recognition and phone tracking. Criminological research until now has focused on the emergence of protests or on the risks of those technologies (e.g. privacy, discrimination and freedom of movement concerns). The way in which command posts operators (e.g. police executives, dispatchers, and government officials) manage such (mediatised) protests and the role played by technologies in those practices of protest management, however, has remained understudied. This study will address these gaps by an empirical research consisting of 35 case studies of Belgian protests. Those case studies will be analysed using the crisis management framework of Boin et al. (2016). Specifically, the study aims to understand how command post operators implement the five tasks of 'sense-making', 'decision-making', 'meaning-making', 'ending and accountability' and 'learning', and what role technologies play in those practices. To this end, the case studies will combine interviews, observations in the command post and document analysis.

[1] "Project number" refers to the institutional project number. This question is optional since not every institution has an internal project number different from the GrantID. Applicants can only provide one project number.

[2] Funder(s) GrantID refers to the number of the DMP at the funder(s), here one can specify multiple GrantIDs if multiple funding sources were used.

[3] Research Organization Registry Community. https://ror.org/

2. Research Data Summary

List and describe all datasets or research materials that you plan to generate/collect or reuse during your research project. For each dataset or data type (observational, experimental etc.), provide a short name & description (sufficient for yourself to know what data it is about), indicate whether the data are newly generated/collected or reused, digital or physical, also indicate the type of the data (the kind of content), its technical format (file extension), and an estimate of the upper limit of the volume of the data[4].

				ONLY FOR DIGITAL DATA	*ONLY FOR DIGITAL DATA*	*ONLY FOR DIGITAL DATA*	*ONLY FOR PHYSICAL DATA*
Dataset Name	Description	New or Reused	Digital or Physical	Digital Data Type	Digital Data Format	Digital Data Volume (MB, GB, TB)	Physical Volume
WP 2: Quantitative survey	Online quantitative survey regarding the use of technologies (for public order policing) in Belgian police forces	☒ Generate new data ☐ Reuse existing data	☒ Digital ☐ Physical	☒ Observational ☐ Experimental ☐ Compiled/ aggregated data ☐ Simulation data ☐ Software ☐ Other ☐ NA	☐ .por ☐ .xml ☐ .tab ☐ .csv ☒ .pdf ☒ .txt ☐ .rtf ☐ .dwg ☐ .tab ☐ .gml ☒ other: .sav,.qsf, .docx ☐ NA	☐ < 100 MB ☒ < 1 GB ☐ < 100 GB ☐ < 1 TB ☐ < 5 TB ☐ < 10 TB ☐ < 50 TB ☐ > 50 TB ☐ NA	
WP 2: Preliminary interviews	Preliminary interviews regarding the (use of technologies for	☒ Generate new data ☐ Reuse existing data	☒ Digital ☒ Physical	☒ Observational ☐ Experimental ☐ Compiled/ aggregated data ☐ Simulation data	☐ .por ☐ .xml ☐ .tab ☐ .csv ☒ .pdf	☒ < 100 MB ☐ < 1 GB ☐ < 100 GB ☐ < 1 TB ☐ < 5 TB	Signed informed consent forms – max. 25 forms (3 pages)

[4] Add rows for each dataset you want to describe.

	the) management of protests			☐ Software ☐ Other ☐ NA	☒ .txt ☐ .rtf ☐ .dwg ☐ .tab ☐ .gml ☒ other: .nvp (NVivo), .docx ☐ NA	☐ < 10 TB ☐ < 50 TB ☐ > 50 TB ☐ NA	
WP 2: exploratory observations	Data from exploratory on-the-job observations in police forces/ command posts regarding the (use of technologies for the) management of protests	☒ Generate new data ☐ Reuse existing data	☒ Digital ☒ Physical	☒ Observational ☐ Experimental ☐ Compiled/ aggregated data ☐ Simulation data ☐ Software ☐ Other ☐ NA	☐ .por ☐ .xml ☐ .tab ☐ .csv ☒ .pdf ☒ .txt ☐ .rtf ☐ .dwg ☐ .tab ☐ .gml ☒ other: .nvp (NVivo), .docx ☐ NA	☒ < 100 MB ☐ < 1 GB ☐ < 100 GB ☐ < 1 TB ☐ < 5 TB ☐ < 10 TB ☐ < 50 TB ☐ > 50 TB ☐ NA	Possibly hand-written observational notes (although preference for digital notes) – one A4 notebook Signed informed consent forms – max. 25 forms (3 pages)
WP 3: case study interviews	Data from case study interviews regarding the (use of technologies for the) management of protests	☒ Generate new data ☐ Reuse existing data	☒ Digital ☒ Physical	☒ Observational ☐ Experimental ☐ Compiled/ aggregated data ☐ Simulation data ☐ Software ☐ Other ☐ NA	☐ .por ☐ .xml ☐ .tab ☐ .csv ☒ .pdf ☒ .txt ☐ .rtf ☐ .dwg ☐ .tab ☐ .gml	☒ < 100 MB ☐ < 1 GB ☐ < 100 GB ☐ < 1 TB ☐ < 5 TB ☐ < 10 TB ☐ < 50 TB ☐ > 50 TB ☐ NA	Signed informed consent forms – max. 50 forms (3 pages)

					☒ other: .nvp (NVivo), .docx ☐ NA		
WP 3: case study observations	Data from on-the-job observations in police forces/ command posts regarding the (use of technologies for the) management of protests	☒ Generate new data ☐ Reuse existing data	☒ Digital ☒ Physical	☒ Observational ☐ Experimental ☐ Compiled/ aggregated data ☐ Simulation data ☐ Software ☐ Other ☐ NA	☐ .por ☐ .xml ☐ .tab ☐ .csv ☒ .pdf ☒ .txt ☐ .rtf ☐ .dwg ☐ .tab ☐ .gml ☒ other: .nvp (NVivo), .docx ☐ NA	☒ < 100 MB ☐ < 1 GB ☐ < 100 GB ☐ < 1 TB ☐ < 5 TB ☐ < 10 TB ☐ < 50 TB ☐ > 50 TB ☐ NA	Possibly hand-written observational notes (although preference for digital notes) – one A4 notebook Signed informed consent forms – max. 75 forms (3 pages)
WP 3: document analysis	Data from selected (police) documents regarding the (use of technologies for the) management of protests	☒ Generate new data ☐ Reuse existing data	☒ Digital ☒ Physical	☒ Observational ☐ Experimental ☐ Compiled/ aggregated data ☐ Simulation data ☐ Software ☐ Other ☐ NA	☐ .por ☐ .xml ☐ .tab ☐ .csv ☒ .pdf ☒ .txt ☐ .rtf ☐ .dwg ☐ .tab ☐ .gml ☒ other: .nvp (NVivo), .docx ☐ NA	☐ < 100 MB ☒ < 1 GB ☐ < 100 GB ☐ < 1 TB ☐ < 5 TB ☐ < 10 TB ☐ < 50 TB ☐ > 50 TB ☐ NA	Possibly the (copies of) physical documents that are selected for analysis – unknown volume

GUIDANCE: *DATA CAN BE DIGITAL OR PHYSICAL (FOR EXAMPLE BIOBANK, BIOLOGICAL SAMPLES, …). DATA TYPE: DATA ARE OFTEN GROUPED BY TYPE (OBSERVATIONAL, EXPERIMENTAL ETC.), FORMAT AND/OR COLLECTION/GENERATION METHOD.* *EXAMPLES OF DATA TYPES: OBSERVATIONAL (E.G. SURVEY RESULTS, SENSOR READINGS, SENSORY OBSERVATIONS); EXPERIMENTAL (E.G. MICROSCOPY, SPECTROSCOPY, CHROMATOGRAMS, GENE SEQUENCES); COMPILED/AGGREGATED DATA[5] (E.G. TEXT & DATA MINING, DERIVED VARIABLES, 3D MODELLING); SIMULATION DATA (E.G. CLIMATE MODELS); SOFTWARE, ETC.* *EXAMPLES OF DATA FORMATS: TABULAR DATA (.POR,. SPSS, STRUCTURED TEXT OR MARK-UP FILE XML, .TAB, .CSV), TEXTUAL DATA (.RTF, .XML, .TXT), GEOSPATIAL DATA (.DWG,. GML, ..), IMAGE DATA, AUDIO DATA, VIDEO DATA, DOCUMENTATION & COMPUTATIONAL SCRIPT.* *DIGITAL DATA VOLUME: PLEASE ESTIMATE THE UPPER LIMIT OF THE VOLUME OF THE DATA PER DATASET OR DATA TYPE.* *PHYSICAL VOLUME: PLEASE ESTIMATE THE PHYSICAL VOLUME OF THE RESEARCH MATERIALS (FOR EXAMPLE THE NUMBER OF RELEVANT BIOLOGICAL SAMPLES THAT NEED TO BE STORED AND PRESERVED DURING THE PROJECT AND/OR AFTER).*

If you reuse existing data, please specify the source, preferably by using a persistent identifier (e.g. DOI, Handle, URL etc.) per dataset or data type.	NA
Are there any ethical issues concerning the creation and/or use of the data (e.g. experiments on humans or animals, dual use)? If so, please describe these issues further and refer to specific datasets or data types when appropriate.	☒ Yes, human subject data ☐ Yes, animal data ☐ Yes, dual use ☐ No If yes, please describe: This study will process several types of personal data (see below). Ethical approval (SMEC) for this study is already obtained (G-2022-5293-R2(MIN)).
Will you process personal data[6]? If so, briefly describe the kind of personal data you will use. Please refer to specific datasets or data types when appropriate. If available, add the reference to your file in your host institution's privacy register.	☒ Yes ☐ No If yes: Ethical approval (SMEC) for this study is already obtained (G-2022-5293-R2(MIN)).

[5] These data are generated by combining multiple existing datasets.

[6] See Glossary Flemish Standard Data Management Plan

	1) From the participants in the online questionnaire – in this case employees (possibly including officers, management and supporting staff) of local police forces in Belgium – diverse data will be processed: specifically their name and e-mail address, the name of the police force and data concerning the implementation of technologies (for public order policing) within the police force. (2) From the participants in the exploratory observations, the preliminary interviews and the case study observations and interviews – in this case employees (possibly including officers, management and supporting staff) of both the local and the federal police in Belgium, non-police command post operators (e.g. government officials) and other informants (e.g. police experts) –, various data will be asked for in interviews and/or observed. Specifically, besides personal information such as their names, occupation and work-experience, the way they manage protests and adopt technologies to this end, and their attitudes towards protest management practices and conditions, such as technologies, that play a role in these practices, will be analysed. If the participants indicate that they want to receive a pdf of the final dissertation of the study, their e-mail addresses will additionally be collected. Similar (personal) data may also be described in the documents (of the police force) that are part of the document analysis. (3) From citizens, only data concerning the specific situation in which their movements or actions influence command post operators' protest management practices will be processed and analysed in a non-individual manner. Names of citizens (including those whose criminal offences are discussed) that are mentioned during the questionnaire, interviews, observations or document analysis will never be mentioned in transcripts, field notes and the report.
Does your work have potential for commercial valorization (e.g. tech transfer, for example spin-offs, commercial exploitation, …)? If so, please comment per dataset or data type where appropriate.	☐ Yes ☒ No If yes, please comment:

Do existing 3rd party agreements restrict exploitation or dissemination of the data you (re)use (e.g. Material/Data transfer agreements, research collaboration agreements)? If so, please explain to what data they relate and what restrictions are in place.	☒ Yes ☐ No If yes, please explain: Following the KU Leuven research collaboration agreement guidelines, the researcher has signed research collaboration agreements with several Belgian police forces that state that confidential information, that is confidential because of the nature of the information, such as data that can lead to the identification of the participants, or because it is marked as confidential by the police force, cannot be shared. To this end, the researcher and the police forces have agreed that the researcher will submit for review any work that is meant for publication so that confidential information can be removed. The police force has a period of ten working days to review the submission. This rule does not apply for the quantitative survey, as this falls outside the scope of the research collaboration agreements.
Are there any other legal issues, such as intellectual property rights and ownership, to be managed related to the data you (re)use? If so, please explain to what data they relate and which restrictions will be asserted.	☐ Yes ☒ No If yes, please explain:

3. Documentation and Metadata	
Clearly describe what approach will be followed to capture the accompanying information necessary to keep **data understandable and usable**, for yourself and others, now and in the future (e.g. in terms of documentation levels and types required, procedures used, Electronic Lab Notebooks, README.txt files, Codebook.tsv etc. where this information is recorded).	(1) For the online quantitative survey data regarding the use of technologies (for public order policing) in Belgian police forces (WP 2), general information on the methodology and informed consent procedure is described in detail in the PRET application (including a draft of the survey and the survey guideline). Furthermore, information about the survey (e.g. the rules about pseudonymisation) and instructions for the participants (e.g. the participant's right to stop the interview or skip a question at any time) are included in the survey guide, together with the survey questions. Moreover, a codebook with variable-level information (including the questions associated with a specific variable number and label, and possible answers associated with values and value labels) will be created and saved as a README.txt file. This codebook will be based on the one made by a colleague (Lore Rooseleers) with the same supervisor for a similar survey (regarding the use of technologies, especially the Focus app, in local police forces in Flanders). (2) For the exploratory and case study interviews (WP 2 & WP3), general information on the methodology and informed consent procedure is described in detail in the PRET application (including a draft of the interview and the interview guideline). Furthermore, information about the interview (e.g. the recording of the interview or rules about pseudonymisation) and instructions for the interviewer and the participants (e.g. the participant's right to stop the interview or skip a question at any time) are included in the interview guide, together with the interview questions and the topic list. Moreover, details about the setting and context of the interview, including the time, place and date of the interview and personal pseudonymised data of the participant, will be documented in digital field notes or the digital transcription of physical field notes. A separate password-protected document (stored away from any folder containing research data) will also be drawn up to keep track of the participants' true identities and the pseudonyms that are used in the study. Next, a separate README.txt file will be created with the rules concerning the transcription of the data. Finally, during the data-analysis in NVivo, a coding structure will be drawn up with variable-level information (main and subcodes and their frequencies) and explanatory comments will be added to these codes in NVivo. In order to keep track of the changes in the coding structure throughout the data-analysis, NVivo recovery files will be created and a separate Word-file will be used to provide an overview of the coding structure with the changes that were made, including the date of the changes and the corresponding recovery file. (3) For the exploratory and case study observations (WP 2 & WP3), general information on the methodology and informed consent procedure is described in detail in the PRET application. Furthermore, information about the observations (e.g. rules about pseudonymisation) is included in the informed consent forms. Moreover, details about

	the setting and context of the observation, including the time, place and date of the observation and personal pseudonymised data of the participants, will be documented in digital field notes or the digital transcription of physical field notes. A separate password-protected document (stored away from any folder containing research data) will also be drawn up to keep track of the participants' true identities and the pseudonyms that are used in the study. Next, a separate README.txt file will be created with the rules concerning the transcription of the data. Finally, during the data-analysis in NVivo, a coding structure will be drawn up with variable-level information (main and subcodes and their frequencies) and explanatory comments will be added to these codes in NVivo. In order to keep track of the changes in the coding structure throughout the data-analysis, NVivo recovery files will be created and a separate Word-file will be used to provide an overview of the coding structure with the changes that were made, including the date of the changes and the corresponding recovery file. (4) For the document analysis (WP 3), general information on the methodology is described in detail in the PRET application. Furthermore, details about the document, such as its name, place of origin and date of creation, will be documented in digital field notes or the digital transcription of physical field notes. Next, a separate README.txt file will be created with the rules concerning the transcription of the data. Finally, during the data-analysis in NVivo, a coding structure will be drawn up with variable-level information (main and subcodes and their frequencies) and explanatory comments will be added to these codes in NVivo. In order to keep track of the changes in the coding structure throughout the data-analysis, NVivo recovery files will be created and a separate Word-file will be used to provide an overview of the coding structure with the changes that were made, including the date of the changes and the corresponding recovery file.
Will a metadata standard be used to make it easier to **find and reuse the data**? If so, please specify which metadata standard will be used. If not, please specify which metadata will be created to make the data easier to find and reuse. *REPOSITORIES COULD ASK TO DELIVER METADATA IN A CERTAIN FORMAT, WITH SPECIFIED ONTOLOGIES AND VOCABULARIES, I.E. STANDARD LISTS WITH UNIQUE IDENTIFIERS.*	☐ Yes ☒ No If yes, please specify (where appropriate per dataset or data type) which metadata standard will be used: NA If no, please specify (where appropriate per dataset or data type) which metadata will be created: As mentioned above, several types of metadata will be created for the survey, interviews, observations and document analysis: information on the methodology and informed consent procedures, information for the researcher and the participants in the survey or interview guidelines, a codebook for the survey and coding structures in NVivo for the interviews, observations and document analysis, separate README.txt files with the rules concerning the transcription of the data and field notes including information on the context of the data-analysis and the study object/ subject.

4. Data Storage & Back-up during the Research Project	
Where will the data be stored?	Digital and audio-visual data will be archived on the researcher's Bitlocker encrypted laptop in different password-protected files, on the OneDrive linked to the researcher's KU Leuven account, and on secure KU Leuven network drives (J: Drive for general documents that do not include personal or sensitive data that can be useful for other members of the research line). Physical data will be stored in the office of the primary researcher in a locked drawer or cupboard that can only be accessed by the researcher. The audio-recordings of the interviews, which will be used to transcribe the research data, will be transferred to the researcher's laptop and OneDrive account and deleted from the portable audio recorder as soon as possible. When the transcription process is completed, the audio files will be deleted from the laptop and OneDrive account of the researcher. Any physical field notes (made during interviews, observations, or the document analysis) will be photographed/ scanned and transcribed into pass-word protected digital documents, after which the physical copies will be destroyed. Furthermore, physical (copies) of documents of the police forces will be stored in a locked drawer until they are photographed/scanned and transcribed into pass-word protected digital documents, after which the documents will be returned to the police force and the physical copies will be destroyed. Finally, signed physical documents, such as research collaboration agreements or informed consent forms, will also be photographed/ scanned into a secured folder on the researcher's laptop and OneDrive account, and the physical copies will be stored in a locked drawer or cupboard during and after the research.
How will the data be backed up? *WHAT STORAGE AND BACKUP PROCEDURES WILL BE IN PLACE TO PREVENT DATA LOSS? DESCRIBE THE LOCATIONS, STORAGE MEDIA AND PROCEDURES THAT WILL BE USED FOR STORING AND BACKING UP DIGITAL AND NON-DIGITAL DATA DURING RESEARCH.*[7] *REFER TO INSTITUTION-SPECIFIC POLICIES REGARDING BACKUP PROCEDURES WHEN APPROPRIATE.*	Physical data (such as field notes) will be transformed into digital transcripts or scans. Digital and audio-visual data will be archived on the researcher's Bitlocker encrypted laptop in different password-protected files, on the OneDrive linked to the researcher's KU Leuven account, and on secure KU Leuven network drives (J: Drive for general documents that do not include personal or sensitive data that can be useful for other members of the research line). Back-ups for the OneDrive and the network-drives are automated.

[7] Source: Ghent University Generic DMP Evaluation Rubric: https://osf.io/2z5g3/

Is there currently sufficient storage & backup capacity during the project? If yes, specify concisely. If no or insufficient storage or backup capacities are available, then explain how this will be taken care of.	☒ Yes ☐ No If yes, please specify concisely: Given the nature and quantity of the research data, the researcher does not expect to exceed the personal storage capacity and the storage capacity of the KU Leuven network-drives. In the case that this does happen, it is possible to expand the capacity.
How will you ensure that the data are securely stored and not accessed or modified by unauthorized persons? *CLEARLY DESCRIBE THE MEASURES (IN TERMS OF PHYSICAL SECURITY, NETWORK SECURITY, AND SECURITY OF COMPUTER SYSTEMS AND FILES) THAT WILL BE TAKEN TO ENSURE THAT STORED AND TRANSFERRED DATA ARE SAFE.* [7]	Digital and audio-visual data will be archived on the researcher's laptop in different password-protected files, on the OneDrive linked to the researcher's KU Leuven account, and on secure KU Leuven network drives (J: Drive for general documents that do not include personal or sensitive data that can be useful for other members of the research line (or the institute)). The laptop of the researcher is encrypted with Bitlocker Drive Encryption, making the data inaccessible even in unauthorised people would obtain the laptop. Furthermore, only the researcher has access to her KU Leuven password-protected OneDrive account. Moreover, some data is shared on the KU Leuven Drives, which are encrypted and only accessible by the researcher, promotor and other authorised people, who are bound by the rules concerning confidentiality and data protection. Files with (personal) research data will also be stored in multiple files that are protected with varying passwords, and files containing the participants' true identities and their pseudonyms will be saved in a separate password-protected document away from any folders containing research data. Finally, contact details of the participants who have indicated that they may want to participate in future research (at the end of the survey, interviews or observations) will be stored in another password-protected file on the researcher's laptop and OneDrive account and on the KU Leuven network drive (J:) of the research line (protected with a password that only members of the research line know). Contact details of the participants who do not wish to be contacted in future research will be deleted after the practical organisation and completion of the survey, interview or observations. Physical data will be stored in the office of the primary researcher in a locked drawer or cupboard that can only be accessed by the researcher. The audio-recordings of the interviews, which will be used to transcribe the research data, will be transferred to the researcher's laptop and OneDrive account and deleted from the portable audio recorder as soon as possible. When the transcription process is completed, the audio files will be deleted from the laptop and OneDrive account of the researcher. Any physical field notes (made during interviews, observations, or the document analysis) will be photographed/ scanned and transcribed into pass-word protected digital documents, after which the physical copies will be destroyed. Furthermore, physical (copies) of documents of the police forces will be stored in a locked drawer until they are photographed/scanned and transcribed into pass-word protected digital documents, after which the documents will be returned to the police force and the physical copies will be destroyed. Finally, signed physical documents, such as research collaboration agreements or informed consent forms, will also be photographed/ scanned into a secured folder on the researcher's laptop and OneDrive account, and the physical copies will be stored in a locked drawer or cupboard during and after the research.

What are the expected costs for data storage and backup during the research project? How will these costs be covered?	The researcher does not expect any additional costs for data storage. If the (OneDrive) storage capacity needs to be expanded, this cost can be covered by the FWO bench fee.

5. Data Preservation after the end of the Research Project	
Which data will be retained for at least five years (or longer, in agreement with other retention policies that are applicable) after the end of the project? In case some data cannot be preserved, clearly state the reasons for this (e.g. legal or contractual restrictions, storage/budget issues, institutional policies...).	All collected data will be preserved for at least 10 years after the end of the research (in accordance with the KU Leuven RDM policy), with the exception of digital contact details of the participants who have indicated that they do not wish to be contacted in future research, the audio-recordings of the interviews, and the physical field notes and the physical (copies of the) documents of the police force. Contact details of the participants who do not wish to be contacted in future research will be deleted after the practical organisation and completion of the survey, interview or observations. Any physical field notes (made during interviews, observations, or the document analysis) will be photographed/ scanned and transcribed into pass-word protected digital documents, after which the physical copies will be destroyed. Finally, physical (copies) of documents of the police forces will be stored in a locked drawer until they are photographed/scanned and transcribed into pass-word protected digital documents, after which the documents will be returned to the police force and the physical copies will be destroyed.
Where will these data be archived (stored and curated for the long-term)?	For long term preservation, at the end of the study, the raw digital data will be placed on the OneDrive linked to the KU Leuven account of the supervisor and his personal KU Leuven network drive. Physical data that are not destroyed or returned after transcription, such as signed research collaboration agreements and informed consent forms, will be locked in a drawer or cupboard that is used for storage purposes in the office of the supervisor or the researcher.
What are the expected costs for data preservation during the expected retention period? How will these costs be covered?	There are no expected costs.

6. Data Sharing and Reuse	
Will the data (or part of the data) be made available for reuse after/during the project? Please explain per dataset or data type which data will be made available. *NOTE THAT 'AVAILABLE' DOES NOT NECESSARILY MEAN THAT THE DATA SET BECOMES OPENLY AVAILABLE, CONDITIONS FOR ACCESS AND USE MAY APPLY. AVAILABILITY IN THIS QUESTION THUS ENTAILS BOTH OPEN & RESTRICTED ACCESS. FOR MORE INFORMATION: HTTPS://WIKI.SURFNET.NL/DISPLAY/STANDARDS/INFO-EU-REPO/#INFOEUREPO-ACCESSRIGHTS*	☐ Yes, in an Open Access repository ☐ Yes, in a restricted access repository (after approval, institutional access only, …) ☒ No (closed access) ☐ Other, please specify: The data from this study (i.e. survey responses, interview transcripts, field notes, document transcripts and codes) will not be shared due to privacy reasons (in accordance with the research collaboration agreements).
If access is restricted, please specify who will be able to access the data and under what conditions.	Only the researcher, the supervisor and KU Leuven researchers working within the team of the supervisor (possibly including KU Leuven students working under the supervision of the promotor), who are bound by the proposed rules of confidentiality and ethical guidelines, will be able to access the data.
Are there any factors that restrict or prevent the sharing of (some of) the data (e.g. as defined in an agreement with a 3rd party, legal restrictions)? Please explain per dataset or data type where appropriate.	☒ Yes, privacy aspects ☐ Yes, intellectual property rights ☒ Yes, ethical aspects ☐ Yes, aspects of dual use ☐ Yes, other ☐ No If yes, please specify: The research data cannot be shared due to privacy reasons and the research collaboration agreements with the police forces.
Where will the data be made available? If already known, please provide a repository per dataset or data type.	NA

When will the data be made available? *THIS COULD BE A SPECIFIC DATE (DD/MM/YYYY) OR AN INDICATION SUCH AS 'UPON PUBLICATION OF RESEARCH RESULTS'.*	NA
Which data usage licenses are you going to provide? If none, please explain why. *A DATA USAGE LICENSE INDICATES WHETHER THE DATA CAN BE REUSED OR NOT AND UNDER WHAT CONDITIONS. IF NO LICENCE IS GRANTED, THE DATA ARE IN A GREY ZONE AND CANNOT BE LEGALLY REUSED. DO NOTE THAT YOU MAY ONLY RELEASE DATA UNDER A LICENCE CHOSEN BY YOURSELF IF IT DOES NOT ALREADY FALL UNDER ANOTHER LICENCE THAT MIGHT PROHIBIT THAT.* *EXAMPLE ANSWER: E.G. "DATA FROM THE PROJECT THAT CAN BE SHARED WILL BE MADE AVAILABLE UNDER A CREATIVE COMMONS ATTRIBUTION LICENSE (CC-BY 4.0), SO THAT USERS HAVE TO GIVE CREDIT TO THE ORIGINAL DATA CREATORS."* [8]	NA
Do you intend to add a PID/DOI/accession number to your dataset(s)? If already available, please provide it here. *INDICATE WHETHER YOU INTEND TO ADD A PERSISTENT AND UNIQUE IDENTIFIER IN ORDER TO IDENTIFY AND RETRIEVE THE DATA.*	☐ Yes ☒ No If yes:
What are the expected costs for data sharing? How will these costs be covered?	NA

[8] Source: Ghent University Generic DMP Evaluation Rubric: https://osf.io/2z5g3/

7. Responsibilities	
Who will manage data documentation and metadata during the research project?	The researcher (Donatella Van Biervliet), in consultation with the supervisor (Prof. Dr. Jeroen Maesschalck), will be responsible for the management of the (meta)data.
Who will manage data storage and backup during the research project?	The researcher (Donatella Van Biervliet), in consultation with the supervisor (Prof. Dr. Jeroen Maesschalck), will be responsible for the management of the data storage on the internal servers of the university and the researcher's OneDrive account. KU Leuven is responsible for the back-up of the data relating to the study on their servers.
Who will manage data preservation and sharing?	The supervisor (Prof. Dr. Maesschalck) will be responsible for the preservation and sharing of the data (after the study is completed).
Who will update and implement this DMP?	The researcher (Donatella Van Biervliet), in consultation with the supervisor (Prof. Dr. Jeroen Maesschalck), will be responsible for the updates and implementation of this DMP.