DATA MANAGEMENT PLAN

PROJECT: Piracy and its control: assessing harms and appraising counter-piracy efforts across regional contexts

GENERAL INFORMATION: The promoter, Prof. Paoli, will be responsible for the preservation of the data collected during this project and will be assisted by the appointed researcher.

1. Interview Data: Recordings (primary; observational; multimedia) will be stored as MP3 files, and transcripts (primary; observational; textual) as Word files. During WP1-4, we anticipate conducting semi-structured interviews with:

1) Representatives of relevant policy-making bodies in the littoral states and at the relevant supra-national levels, NGOs related to the shipping industry (e.g., International Chamber of Shipping);
2) Harm bearers from each category to include individuals (e.g., seafarers or delegates from their representative organizations), private-sector entities (e.g., vessel owners, shipping firms, private security companies), government entities (e.g., port authorities, maritime police, coast guard and Navy) and the environment (e.g., environmental NGOs and representatives of affected communities).

We will collect the name, e-mail address, and information about the employer/organization the interview participant is involved with. If the interview participants allow it, we will record the interviews, then transcribe the recordings and conduct the analyses. As soon as the interviews have been transcribed (and fully anonymized), the audio recordings will be deleted. A file-shredding application will be utilized to delete the files, effectively writing, deleting and overwriting the data entirely, in order to prevent its recovery.

The digital data from interviews will be stored and modified on network drives, which are encrypted, automatically synchronized, and only be accessible by Paoli and the appointed researcher. These network drives will be back-upped daily. Hence, the digital data will be stored in such a way that loss or misuse is prevented at all times. In addition, each file containing personal data will be encrypted by the KU Leuven IT services using BitLocker Drive Encryption software and will be stored only on a secured cloud to avoid any misuse of the data gathered.

2. Interview Analysis/Output: To include textual analyses (primary; derived; textual) and will be stored as NVIVO files.

This digital data will also be stored and modified on network drives, which are encrypted, automatically synchronized, and only be accessible by Paoli, the co-promotors and the appointed researcher. These network drives will be back-upped daily. Hence, the digital data will be stored in such a way that loss or misuse is prevented at all times.

3. Legal/Document Analysis Output: Textual analyses (primary; derived; textual) will be stored as Word files.

This digital data will also be stored and modified on network drives, which are encrypted, automatically synchronized, and only be accessible by Paoli, the co-promotors and the appointed researcher. These network drives will be back-upped daily. Hence, the digital data will be stored in such a way that loss or misuse is prevented at all times.

4. Manuscripts/Presentations: (primary; derived; textual) will be stored as Word and PowerPoint files, respectively.

This digital data will also be stored and modified on network drives, which are encrypted, automatically synchronized, and only be accessible by Paoli, the co-promotors and the appointed researcher. These network drives will be backed-up daily. Hence, the digital data will be stored in such a way that loss or misuse is prevented at all times.

5. Datasets: Piracy incident datasets will be created, maintained and manipulated in Excel and/or SPSS file format.

This digital data will also be stored and modified on network drives, which are encrypted, automatically synchronized, and only be accessible by Paoli and the appointed researcher. These network drives will be back-upped daily. Hence, the digital data will be stored in such a way that loss or misuse is prevented at all times.

6. Paper Data/Files/Documents: Although we will strive to reduce the amount of paper documents, any such data will be stored in file boxes, which will be put in a closet and/or file cabinet in the office of the researcher hired for this project. This closet (and/or file cabinet) will be locked every time the researcher leaves the office. In such a way, the loss or misuse of the paper is prevented. Only the researcher and the promoter will possess keys to the closet (and/or file cabinet). Any paper files no longer needed (or after they have been digitized) will be destroyed utilizing a paper shredder, the by-product disposed of appropriately.

ADDITIONAL INFORMATION:

Data Storage/Management at the University of Bristol: Any digital project data/files stored at the University of Bristol will also be kept archive network drives, ensuring that they are protected (by encryption), preserved (the drives will be automatically backed-up) and accessible if needed. Any paper files will be stored in a lockable closet/file cabinet in the co-promotor's office. Only the co-promotor will possess a key to the closet/file cabinet. Any paper files no longer needed (or after they have been digitized) will be destroyed utilizing a paper shredder, the by-product disposed of appropriately.

Upon Project Completion: After the project has been completed, the data emerging from interview and document analysis will be stored on archive network drives, ensuring that they are protected (by encryption), preserved (the drives will be automatically backed-up) and accessible if needed. Respecting the agreements made with the original interviewees, only the promotor and the appointed researcher will have access to such data.

The dataset of the piracy incidents will be stored on the KU Leuven Research Data Repository (https://rdr.kuleuven.be/). It will be stored in Excel format (xls) to increase its accessibility.

All data will be stored for at least ten years.