DATAGOV security workflow_ workshop (early fall 2026)
v 01, prepared by SM
7 July 2026

Goal

- generating and consolidating the **DATAGOV security workflow & risk register** as a living document, to be revised (bi?)annually
- beyond a technical compliance exercise (e.g., GDPR checklist)
- but combining research practices ("how to"), security (and cybersecurity), data governance, research ethics, critical analysis of our research infrastructure, and mitigation strategies.

Deliverables (*internal)

1. security workflow (narrative, ~5-8 pages to be included also in the Ethics WP, the only public-facing deliberable from this process)
2. risk register (in the form of a spreadsheet)
3. data classification policy (for each type of data, define level of security)
4. access matrix (who has access to what, when, wherem and with what level of permission)
5. incident response procedure (1 page: what to do if/when shit happens)
6. new team member onboarding checklist

Process
In six steps; the first three are described below.

Overview of steps (note → documentation throughout):

1. inventory of DATAGOV "assets"
2. workflow/life cycle of data
3. great modelling
4. definition of shared security rules
5. assign roles and responsibilities
6. incident workflow

In an ideal situation, we would meet as a group. Given there is the summer inbetween and Mattéo will soon go to the field, my proposal is to twist the process. I therefore ask each of you to do some homework individually.

Individual assignments are marked in yellow; prepare to share in our upcoming workshop.

Deadine for individual assignments: **August 30** (for a workshop early September).
TO DO: share ONLY table (step 1) and scenarios (step 3) with Stefi; bring the rest to the workshop

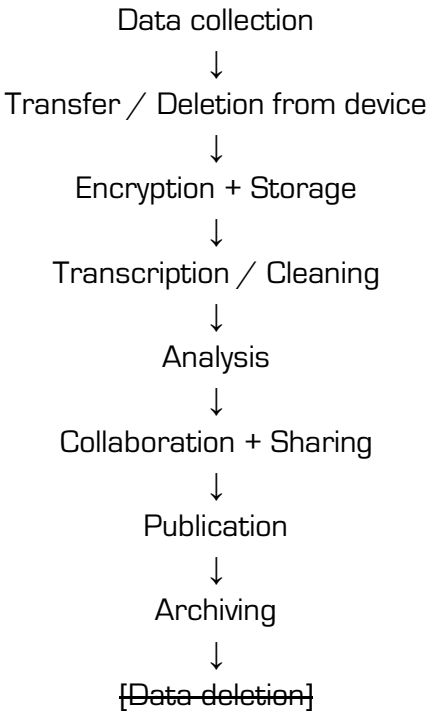
STEP 1: THE INVENTORY: MAP WHAT NEEDS PROTECTING

TASK: Compile the table (think of all data potentially gathered within DATAGOV, not just your own projcet). Spme basic examples are included; please expand ect.

asset	in DATAGOV	risk if compromised
Research data	Interviews fieldwork notes	Privacy breach GDPR violation
People	Research participants: Researchers	
Infrastructure		
Knowledge	Coding schemes Unpublished writings Game prompts	
Software		

STEP 2: MAP THE WORKFLOW/LIFE CYCLE OF EACH ASSET

Example:



TASK: For each type of data, and for each step ask:

- who has access?
- where is the data?
- is it encrypted/in a safe space?
- what could go wrong? (doom scenarios welcome)
- what is our mitigation?
-

Take notes (to share in our upcoming workshop)

Step 3: THREAT MODELLING

TASK: Generating *realistic scenarios* based on YOUR concrete research plans **in the next 12 months**. In other words, identify plausible threats that may affect your research activities, data, participants, or the project/team as a whole.
Note down

- what data will you collect? (include also the methods)
- who will you interact with?
- where/how is the interaction taking place?
- what digital tools or infrastructures will you use?

Examples of threats:

- phishing email steals a UvA password.
- lost laptop, stolen recorder
- data transfer across border with data on personal devices
- student assistant downloads participant data onto a personal computer.
- malicious actors attempt to obtain sensitive interview data

For every threat record (e.g.):

- likelihood
- impact
- mitigation
- responsible person

It is also worth asking ourselves:

- who becomes visible through this process/infrastructure?
- who is rendered invisible?
- could security measures themselves produce exclusion or create barriers for vulnerable groups (e.g., contact interviewees on Signal when they use Whatsapp)?
- what new dependencies are created?
- are research subjects able to contest decisions based on our workflow?
- what assumptions are embedded in the data model?

Fill the table (the example is deliberately wrong):

Threat scenario	What could happen?	Likelihood (L/M/H)	Impact (L/M/H)	Existing safeguards	Additional mitigation
My laptop is stolen while travelling for fieldwork.	Interview transcripts become inaccessible or exposed.	Medium	High	Disk encryption, password	Enable remote wipe and avoid storing raw recordings locally.