Workshop on documentation under the “new 45”: Scenario “DEMIGOD”

Your EUI wants to develop a system called the **D**igital **E**uropean **M**illennium **I**ntegrated **G**rant **O**versight **D**atabase (DEMIGOD). Assume that the EUI Regulation provides a defensible legal basis for doing so. EUI will use DEMIGOD for managing research and development grants for research entities and SMEs (legal entities). However, grant applications fed into DEMIGOD also include detailed information on lead researchers and other beneficiary staff (e.g. CVs). MS authorities will use DEMIGOD for managing national grants, too. EUI management would like to provide DEMIGOD as a service to other EUIs.

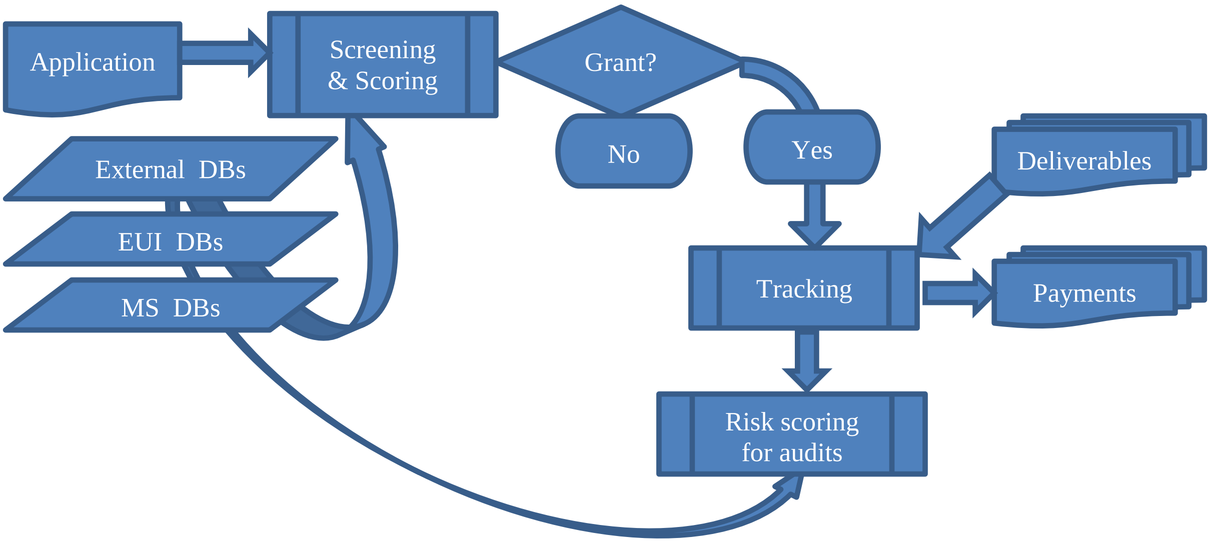
DEMIGOD covers the entire lifecycle of grants. The system uses proprietary software developed by an external vendor, which also runs DEMIGOD in its European cloud environment.

DEMIGOD helps EUI decide whom to give grants by automatically screening applications: checking completeness, aggregating information on past grants to recipients and the results obtained, checking citation databases for scientific impact and scoring researchers accordingly, as well as checking exclusions due to past irregularities. DEMIGOD connects to external information providers, to EUI’s older systems replaced by it, and to Member States’ own systems[1]. Based on all this, the system automatically scores researchers to assist grant managers in their selection decisions on award of a new grant with a traffic light system

DEMIGOD also tracks payments and deliverables.

Finally, DEMIGOD also helps in selecting targets for auditing or ex-post checks. To do so, it generates an automatic risk score, based on past findings involving the same researchers or their affiliated institutions. It also takes into account commercial business intelligence databases (tracking e.g. whether grantees have been the subject of “adverse media coverage”).

The project owner has provided you a first draft of a data flow diagram:



[1] One of the reasons in the business case for DEMIGOD is the case of a network of professors notorious for creative accounting applying for countless grants in different MS, which did not know of their history in other MS. One of DEMIGOD’s aims is to prevent such cases from reoccurring.

Together with the project owner, you have already determined that DEMIGOD requires a DPIA (criteria 1, 2, 8 at least). Now, the project owner approaches you for guidance on how to assess the risks to data subject in the “screening & scoring” and “tracking” sub-processes.

Exercise: Below, you will find the guiding questions from the draft documentation guidance. How would you use them to help the project owner go in the right direction?

Guiding Questions on fairness

- Can people expect this to happen, also if they don’t read the information you provide them with?
- In case you rely on consent, is it really free? How do you document that people gave it? How can they revoke their consent?
- Could this generate chilling effects?
- Could this lead to discrimination?
- Is it easy for people to exercise their rights to access, rectification, etc.?

Guiding Questions on transparency

- How will you tell people about your processing?
- How do you make sure the information reaches the persons affected?
- Is the information you provide complete and easy to understand?
- Is it targeted to the audience? E.g. children may require tailored information
- In case you defer informing people, how do you justify this?

Guiding Questions on purpose limitation

- Have you identified all purposes of your process?
- Are all purposes compatible with the initial purpose?
- Is there a risk that the data could be reused for other purposes (function creep)?
- How can you ensure that data are only used for their defined purposes?
- In case you want to make available / re-use data for scientific research, statistical or historical purposes, what safeguards do you apply to protect the individuals concerned?

Guiding Questions on data minimisation

- Are the data of sufficient quality for the purpose?
- Do the data you collect measure what you intend to measure?
- Are there data items you could remove without compromising the purpose of the process?
- Do you clearly distinguish between mandatory and optional items in forms?
- In case you want to keep information for statistical purposes, how do you manage the risk of re-identification?

Guiding Questions on accuracy

- What could be the consequences for the persons affected of acting on inaccurate information in this process?
- How do you ensure that the data you collect yourself are accurate?
- How do you ensure that data you obtain from third parties are accurate?
- Do your tools allow updating / correcting data where necessary?
- Do your tools allow consistency checks?

Guiding Questions on storage limitation

- Does EU legislation define storage periods for your process?
- How long do you need to keep which data? For which purpose(s)?
- Can you distinguish storage periods for different parts of the data?
- If you cannot delete the data just yet, can you restrict access to it?
- Will your tools allow automated erasure at the end of the storage period?

Guiding Questions on security

- Do you have a procedure to perform an identification, analysis and evaluation of the information security risks possibly affecting personal data and the IT systems supporting their processing?
- Do you target the impact on people’s fundamental rights, freedoms and interests and not only the risks to the organisation?
- Do you take into consideration the nature, scope, context and purposes of processing when assessing the risks?
- Do you manage your system vulnerabilities and threats for your data and systems?
- Do you have resources and staff with assigned roles to perform the risk assessment?