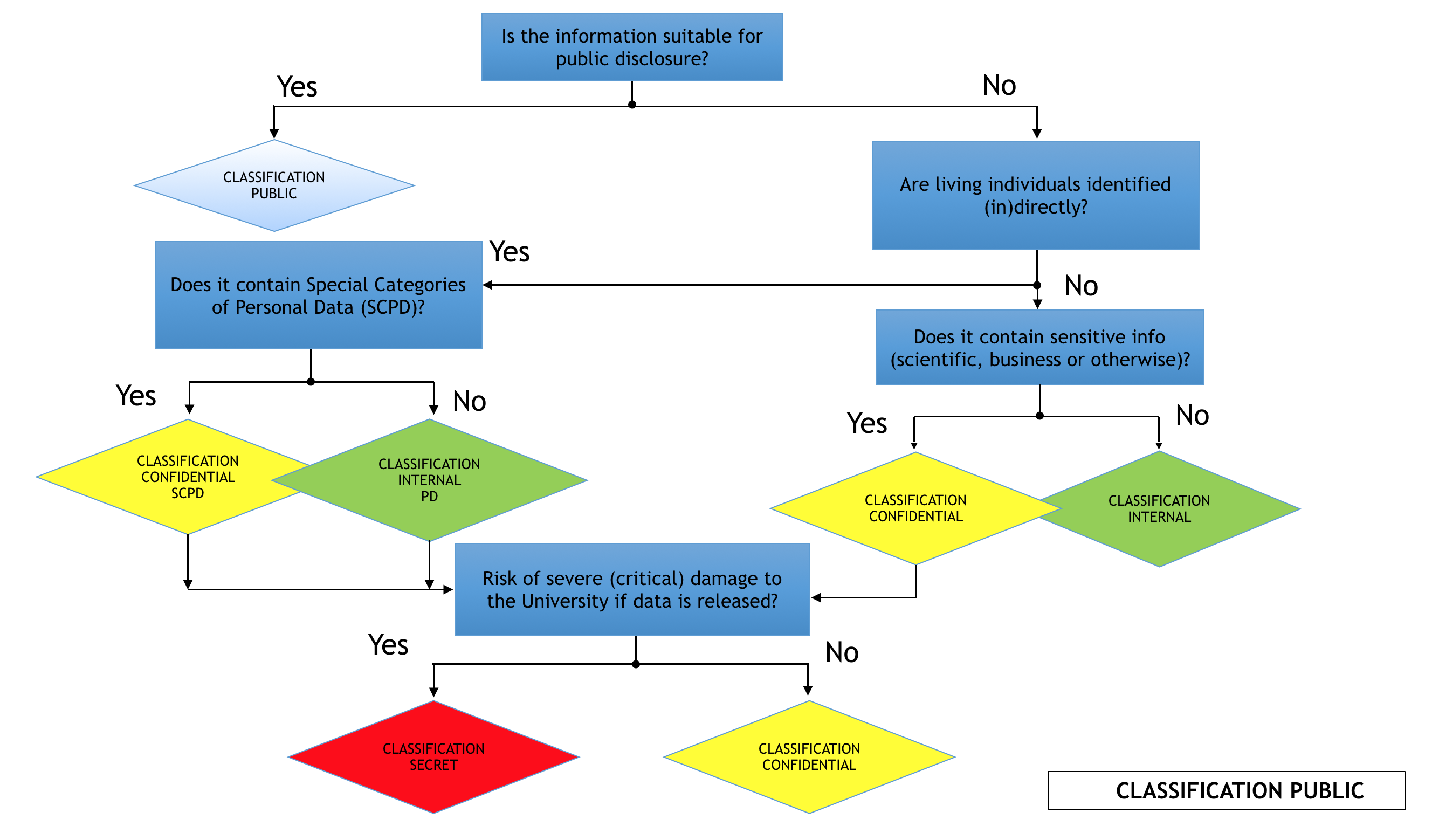
|  | CLASSIFICATION PUBLIC | CLASSIFICATION INTERNAL (\*PD) | CLASSIFICATION CONFIDENTIAL (\*SCPD) | CLASSIFICATION SECRET |
| --- | --- | --- | --- | --- |
| Level of Need-To-Know | May be viewed by all members of the public | May be seen by all members of the Erasmus University Rotterdam.  Should be additionally labeled as PD if the document consist Personal Data.    PD may be accessible only by Erasmus University Rotterdam members that have “need-to-know” to process PD.   * (PD) Personal Data | Accessible by restricted members of staff or students, on a “need-to-know” basis.  Should be additionally labeled as SCPD if the document consist Special Categories Personal Data.  SCPD & PD may be accessible only by Erasmus University Rotterdam members that have “need-to-know to process PD or SCPD.  \*(SCPD) Special Categories Personal Data | Accessible only to designated or relevant members of staff or scientists, due to its potential critical impact on the Erasmus University Rotterdam, including critical financial or critical reputational damage. |
| Level of risk if released  inappro-priately | None | Low  Should it fall into the wrong hands could be harmful (slightly damaging) to people or organization. | Medium  Should it fall into the wrong hands could cause serious damage to people or organization. | High  Should it fall into the wrong hands could cause severe (critical) damage to people or organisation. |
| Transmission / Transport / Storage / Archiving | No Restrictions | PAPER information must be stored in lockable cabinets and kept from persons that don’t have any “need-to-know” (visitors, cleaners, movers etc...)  Remove sensitive mail content before sending the mail to external organizations (declassify to CLASSIFICATION PUBLIC)  Sending INTERNAL/PD information (documents) outside own organization must be done with Surffilesender.  Use of password is mandatory. Password sharing allowed through the mail.  Sending INTERNAL/PD information to own private email environment is prohibited.  NETWORK Storage: INTERNAL/PD Information must be stored in shared folders with restricted access. | PAPER information must be stored in lockable cabinets and kept from persons that don’t have any “need-to-know” (see INTERNAL, including the co-workers from other departments or units)  Printing CONFIDENTIAL information should be reduced to minimum.  Remove sensitive mail content before sending the mail to external organizations (declassify to CLASSIFICATION PUBLIC)  Sending CONFIDENTIAL/SCPD information (documents) outside own organisation must be done with Surffilesender. Use of password is mandatory. Password sharing only through SMS.  Sending CONFIDENTIAL/SCPD information to own private email environment is prohibited. | PAPER information must be stored in security safe or vault. Need-to-know strictly reserved for a designated few.  Hard copies of documents should be hand delivered internally.  Printing SECRET information should be avoided. Copying SECRET documents should be avoided. Copied or printed documents must be marked with a follow number and registered which recipients received a copy.  Securing the document with the password (encryption) is mandatory. Password sharing only through SMS.  Remove sensitive mail content before sending the mail to external organizations (declassify to CLASSIFICATION PUBLIC) |

**Determining the data classification: decision tree.**