

## Model development

- Data pseudonymisation and anonymisation measures
- Measures to reduce the risk of memorisation



Learning



Does the training dataset contain personal data?

No

Yes

Yes

Is the model specifically designed to provide information about the individuals whose data is contained in the training set, or in a way that makes this data accessible?

No

In most cases, conduct attack tests on the model to determine the likelihood of re-identification of each type of personal training data

Did the model status analysis conclude that the likelihood of re-identification was insignificant for each type of personal data?

Yes

The model is presumed anonymous

No

Data protection rules apply to the model.  
The controller may choose to:

### Apply GDPR

Continue in accordance with the rules on privacy protection.

Refer to the how-to sheets on information, the exercise of rights, and verify the lawfulness of the processing of the model. Reduce the risks of regurgitation and attack, in particular through the measures listed in the sheet.

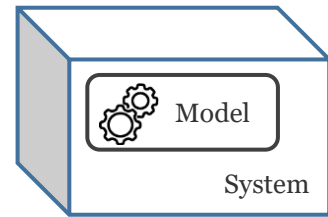
Encapsulate the model in a system that incorporates robust measures to reduce the likelihood of data extraction from the system.

Refer to Figure 2 and the relevant sections of the data sheet.

Document

## Development of an AI system based on a non-anonymous model compliant with the GDPR

- Measures to reduce the likelihood of re-identification from access to the system



In **all cases**, conduct attack tests on the system to determine the likelihood of re-identification of each type of personal training data

Did the analysis of the system status conclude that there is no significant likelihood of re-identification based on the use of the system for each type of personal data?

Yes

Use of the system may be presumed to fall outside the scope of the GDPR

No

Data protection rules apply to the model.

### The GDPR applies

Continue in accordance with the rules on privacy protection.

Refer to the information sheets, the exercise of rights, and verify the lawfulness of the processing of the template. Reduce the risk of regurgitation and attack, in particular through the measures listed in the sheet.

Document