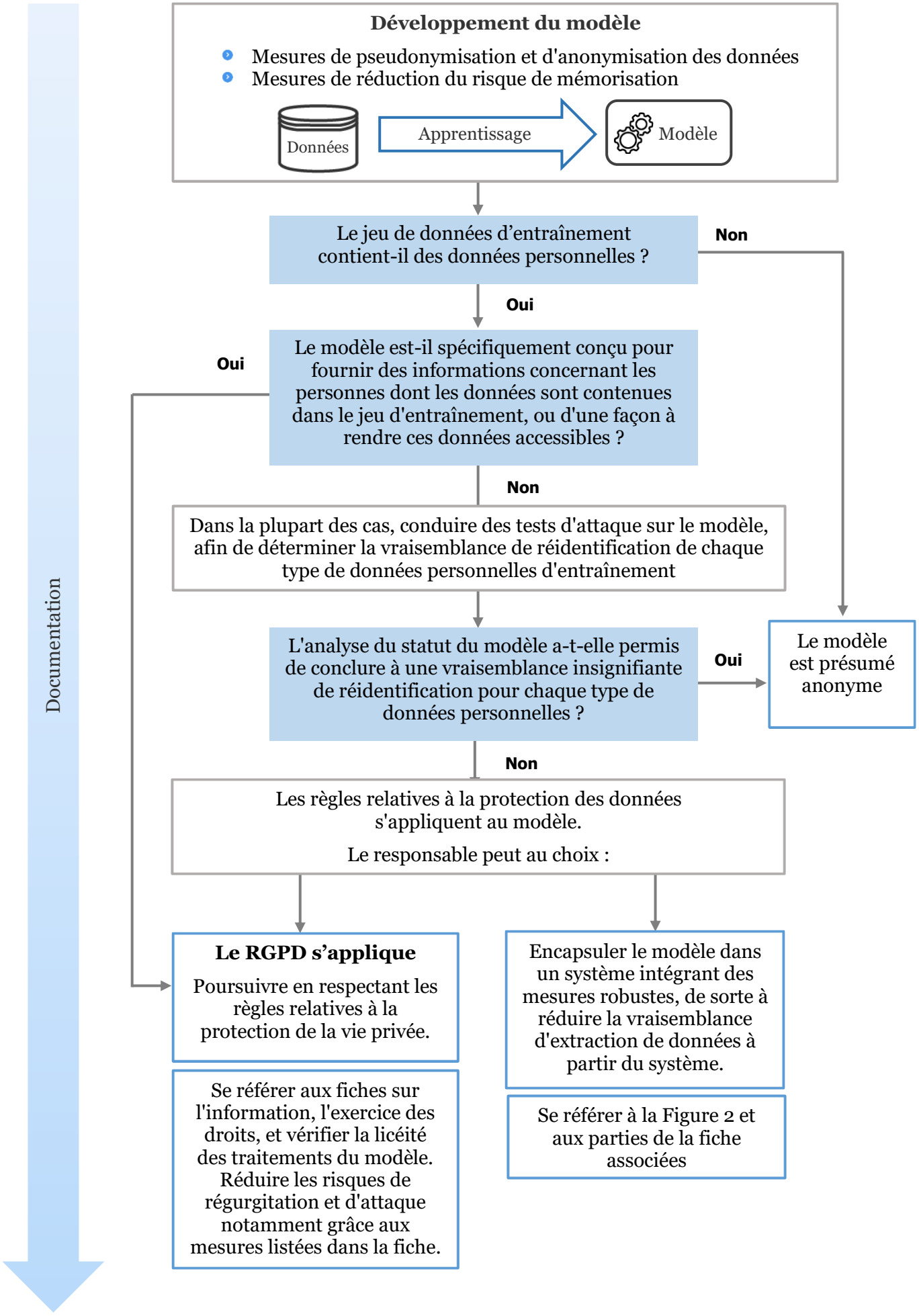
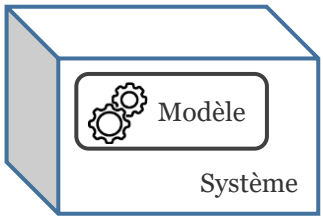

Développement du modèle
Mesures de pseudonymisation et d'anonymisation des données
Mesures de réduction du risque de mémorisation
Données
Apprentissage
Modèle
Le jeu de données d'entraînement contient-il des données personnelles ?
Non
Oui
Le modèle est-il spécifiquement conçu pour fournir des informations concernant les personnes dont les données sont contenues dans le jeu d'entraînement, ou d'une façon à rendre ces données accessibles ?
Oui
Non
Dans la plupart des cas, conduire des tests d'attaque sur le modèle, afin de déterminer la vraisemblance de réidentification de chaque type de données personnelles d'entraînement
L'analyse du statut du modèle a-t-elle permis de conclure à une vraisemblance insignifiante de réidentification pour chaque type de données personnelles ?
Oui
Le modèle est présumé anonyme
Non
Les règles relatives à la protection des données s'appliquent au modèle.
Le responsable peut au choix :
Le RGPD s'applique
Poursuivre en respectant les règles relatives à la protection de la vie privée.
Encapsuler le modèle dans un système intégrant des mesures robustes, de sorte à réduire la vraisemblance d'extraction de données à partir du système.
Se référer aux fiches sur l'information, l'exercice des droits, et vérifier la licéité des traitements du modèle. Réduire les risques de régurgitation et d'attaque notamment grâce aux mesures listées dans la fiche.
Se référer à la Figure 2 et aux parties de la fiche associées
Documentation

Documentation

Développement d'un système d'IA basé sur un modèle non anonyme et conforme au RGPD

- Mesures de réduction de la vraisemblance de réidentification à partir d'un accès au système



Dans **tous** les cas, conduire des tests d'attaque sur le système, afin de déterminer la vraisemblance de réidentification de chaque type de données personnelles d'entraînement

L'analyse du statut du système a-t-elle permis de conclure à une vraisemblance insignifiante de réidentification à partir de l'utilisation du système pour chaque type de données personnelles ?

Oui → L'utilisation du système peut être présumée sortie du champ d'application du RGPD

Non

Les règles relatives à la protection des données s'appliquent au modèle.

Le RGPD s'applique

Poursuivre en respectant les règles relatives à la protection de la vie privée.

Se référer aux fiches sur l'information, l'exercice des droits, et vérifier la licéité des traitements du modèle. Réduire les risques de régurgitation et d'attaque notamment grâce aux mesures listées dans la fiche.