Assistance à l'ingénierie de logiciels pour mieux protéger la vie privée des utilisateurs

Selena Lamari [1,2]

[1] LIRMM, Univ. Montpellier, CNRS, Montpellier, France [2] LRDSI, Univ. Blida 1, Blida, Algeria

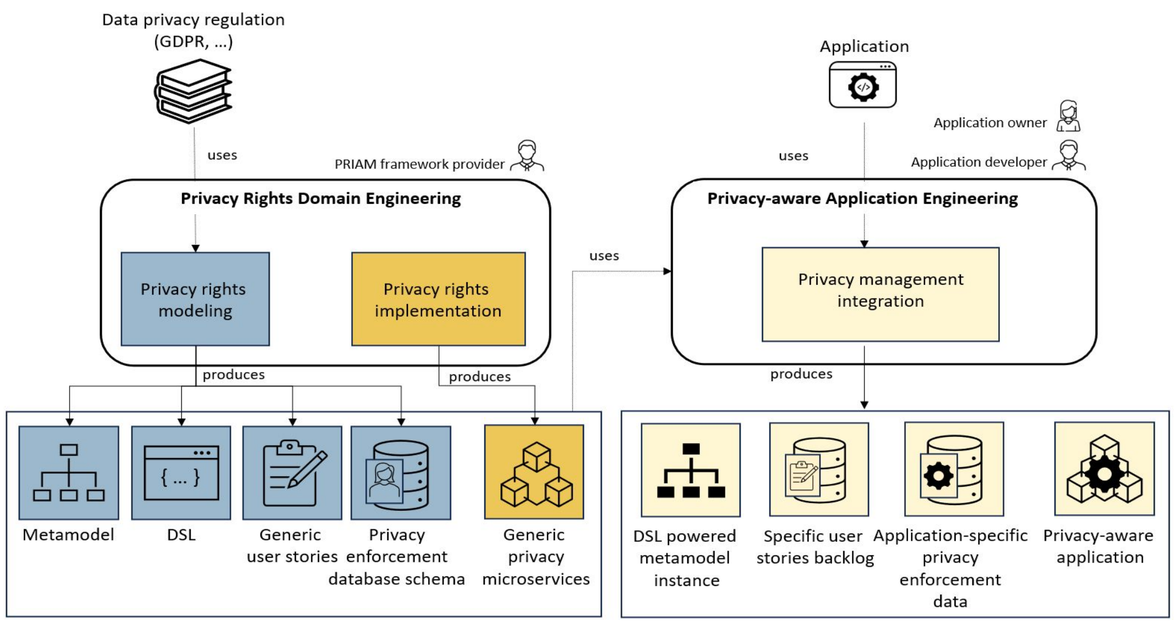
I. Contexte et motivation

- Depuis 2018 : **obligation d'implémenter le RGPD**, règlement européen de protection de la vie privée des utilisateurs par la protection des données personnelles.
- Mise en oeuvre **fastidieuse** pour les développeurs, en raison de la **longueur** et de la **complexité** du texte réglementaire.

Proposition d'une solution assistant les développeurs dans la mise en conformité au RGPD[3] de leurs applications

II. PRIAM : Approche globale à 3 étapes

1. Formaliser les **concepts** d'un **règlement** à l'aide d'un **métamodèle** (Domain Engineering).
2. Fournir des **artéfacts génériques facilitant** l'implémentation des concepts du règlement dans des **applications en cours** de développement ou déjà **existantes** (évolution).
3. Proposer un **processus** et des **outils** permettant d'**adapter** les artéfacts génériques aux besoins spécifiques de chaque application (Application Engineering).

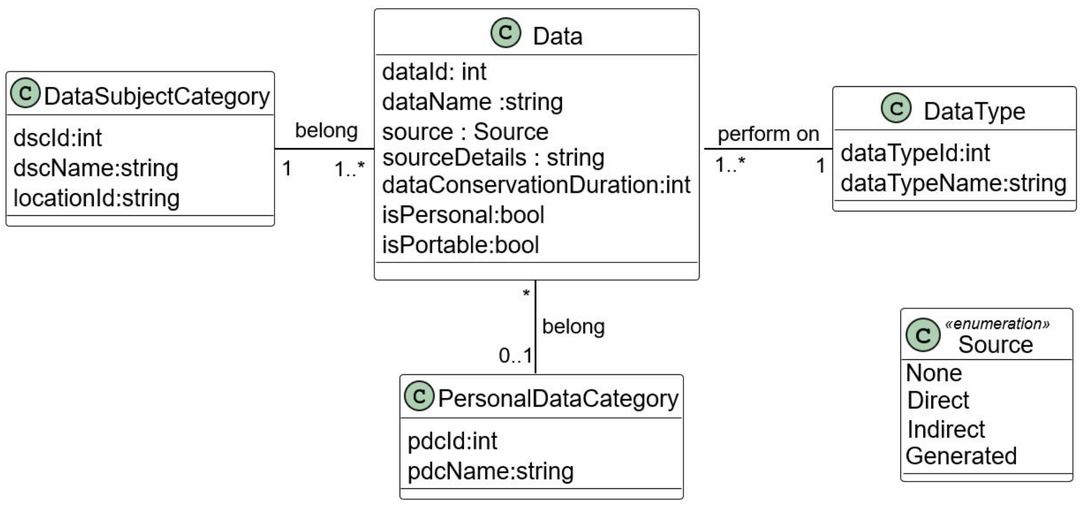


Approche proposée pour l'intégration de la protection de la vie privée

A. Modélisation du droit à la vie privée

1. Conception du métamodèle PRIAM

- Défini à partir du texte **réglementaire de la RGPD.**
- Comprenant **50 classes** regroupées en **7 packages.**
- **Validation qualitative** par des **experts du domaine** (DSI, juristes) en utilisant un **questionnaire** [4] évaluant la conformité au RGPD.



Extrait du métamodèle PRIAM (package "Data")

[3]https://www.cnil.fr/fr/reglement-europeen-protection-donnees

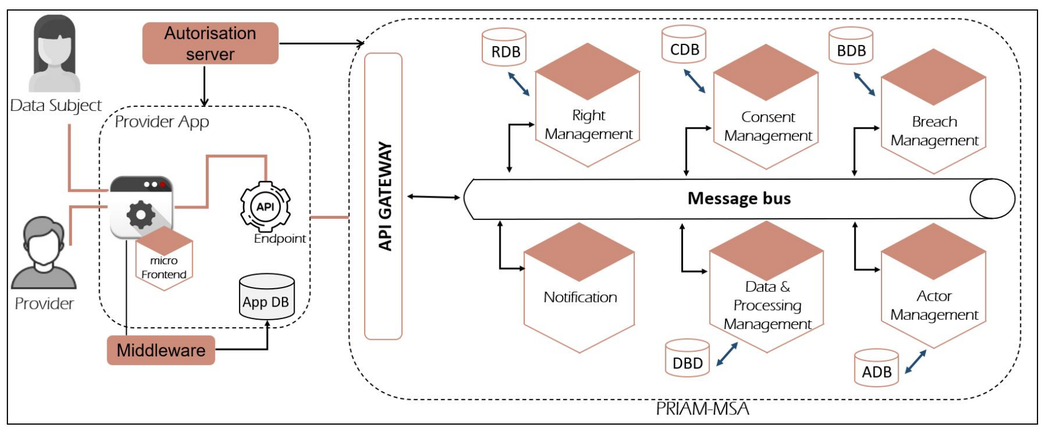
[4]https://www.dataprotection.ie/sites/default/files/uploads/2019-04/A-Guide-to-help-SMEs-Prepare-for-the-GDPR.pdf

2. Conception d'un outillage d'IDM basé sur le métamodèle PRIAM

- **User stories génériques.**
- **Schéma de base de données générique** (BD PRIAM).
- **DSL** permettant d'**adapter** les artéfacts génériques aux **besoins spécifiques des applications.**

B. Implémentation des droits de la protection de la vie privée

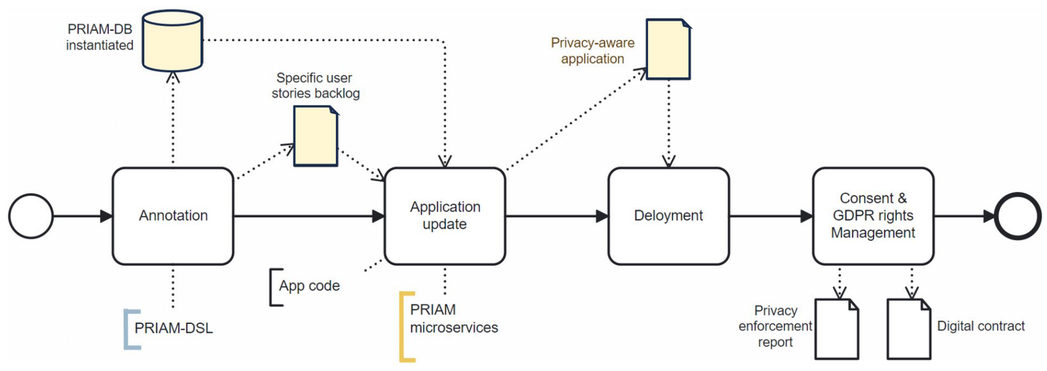
- Basée sur une **architecture à microservices** qui couvre les exigences du RGPD (implémentation des user stories génériques).
- Assure la **gestion d'accès aux données** en se basant sur le **consentement** des utilisateurs (interception des requêtes).
- Intègre un système de **sécurité OAuth2** (SSO) pour la **gestion de l'authentification.**



Architecture à microservices de PRIAM

C. Intégration de la gestion de la vie privée

1. **Annotation** manuelle des données personnelles et de leurs traitements à l'aide du **DSL.**
2. **Génération** automatique des **user stories** spécifiques.
3. **Génération** automatique du **script d'instanciation** spécifique de la **BD PRIAM.**
4. **Intégration** semi-automatique **des micro-services** à l'application en se basant sur les artéfacts spécifiques générés.
5. **Déploiement** de l'application **conforme au RGPD.**



Aperçu du processus de mise en vigueur de la Privacy

PoC sur un **cas d'étude :** application "Tea Store" utilisée comme démonstrateur dans le cadre de l'atelier Cisco Full Stack Observability[5]

III. Perspectives

- Réaliser des **expériences à grande échelle**, sur des applications plus vastes.
- **Généraliser l'approche** pour supporter tout autre règlement ayant un impact sur les exigences d'une application.

[5] https://github.com/DescartesResearch/TeaStore

Contact :
selena.lamari@lirmm.fr