amU
Aix Marseille Université

Institut
Archimède
Mathématiques-Informatique
Aix Marseille Université

Towards Automated Checking of GDPR Compliance

Pauline Di Salvo Cilia, Alba Martinez Anton, Clara Bertolissi

IARIA

Presented by:

Alba Martinez Anton

Aix-Marseille University, CNRS

alba.martinez-anton@lis-lab.fr

LIS
LABORATOIRE
D'INFORMATIQUE
& SYSTÈMES
UMR 7020

Alba Martinez Anton, Phd Student at Aix-Marseille University

Academic background:

- Computer Science PHd student at Aix-Marseille University (since november 2021)
  - Subject: Privacy Protection through the Formalization of Provenance-Based Models.
  - Thesis defense in Decembre 2024
- Masters Computer Science Fiability and Security from Aix-Marseille University (2019-2021)
- International Licence Mathematics and Computer Science from University of Bordeaux (2016 -2019)

Summary

- Definition and context of GDPR compliance
- Extending the Open Provenance Model
- Tool for compliance verification: Architecture and Implementation

Privacy exposition and GDPR

- Increase in the quantity of personal data stored and processed by computer systems in recent years

+

- Abuse of the use of this data: Cambridge Analytica, Facebook-CIA scandal, and the Equifax data breach.

↓

- Emergence of laws regulating the use of personal data, such as the GDPR in the European Union.

GDPR Principles

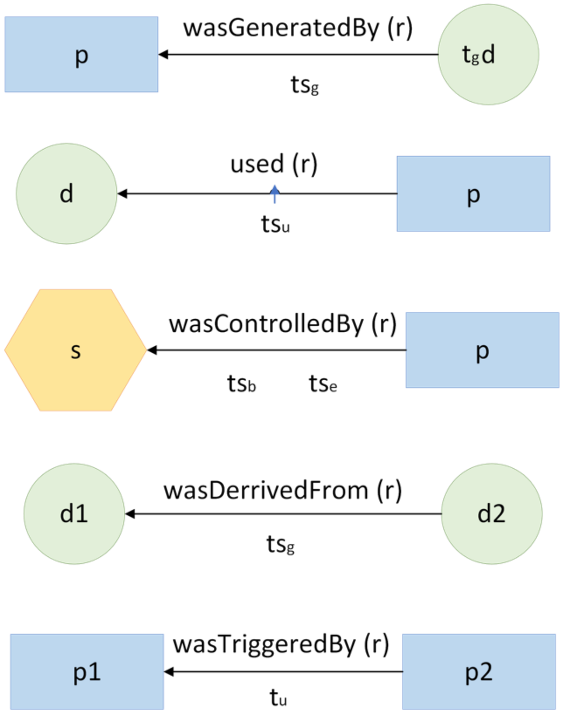
- **Consent compliance [GDPR art.6]** : personal data is used only for purposes the user has given consent to.
- **Data access [GDPR art.15(1)]:** a report is sent *in time* after a user request.
- **Data erasure [GDPR art.17]** : personal data is erased *in time* after a user request.
- **Storage limitation [GDPR art.5(1)]:** personal data must not be stored for *too long* after its last use.

- Automation the compliance verification of the system events?

The Open provenance Model

Representation of the data provenance, through a graph

EFFECT → CAUSE

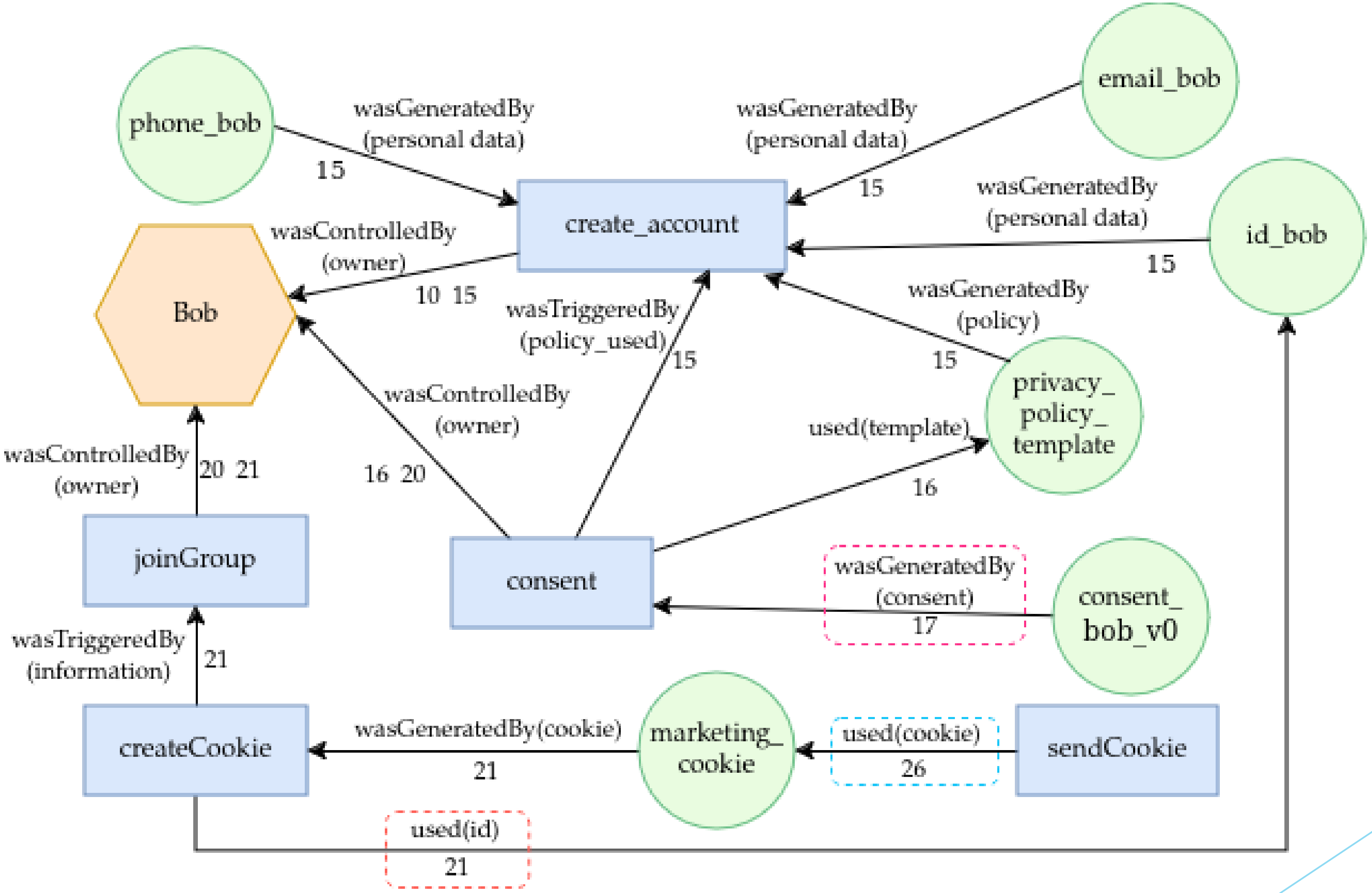


- ○ Two particular artefacts:

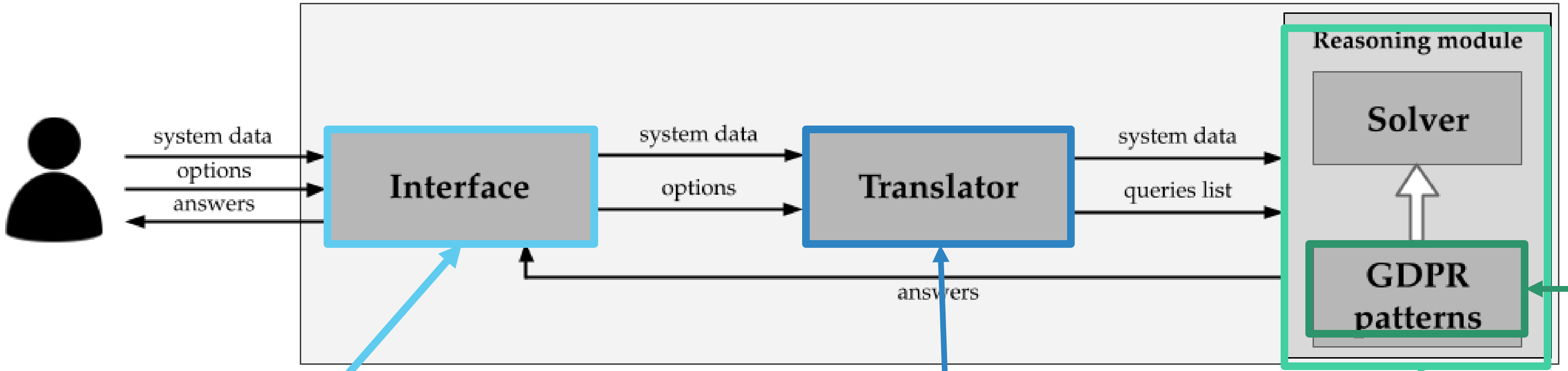
Privacy_policy_templete
consent

- ○ Extension with attributes:
  - ○ Purposes
  - ○ Personal data

A provenance graph exemple



Prototype Architecture



Prolog rules representing GDPR principles

- Specify system data and options
- Display answers

- Convert Interface inputs into Prolog queries

- Resolve path queries and return all possible instanciations

Prototype: an exemple

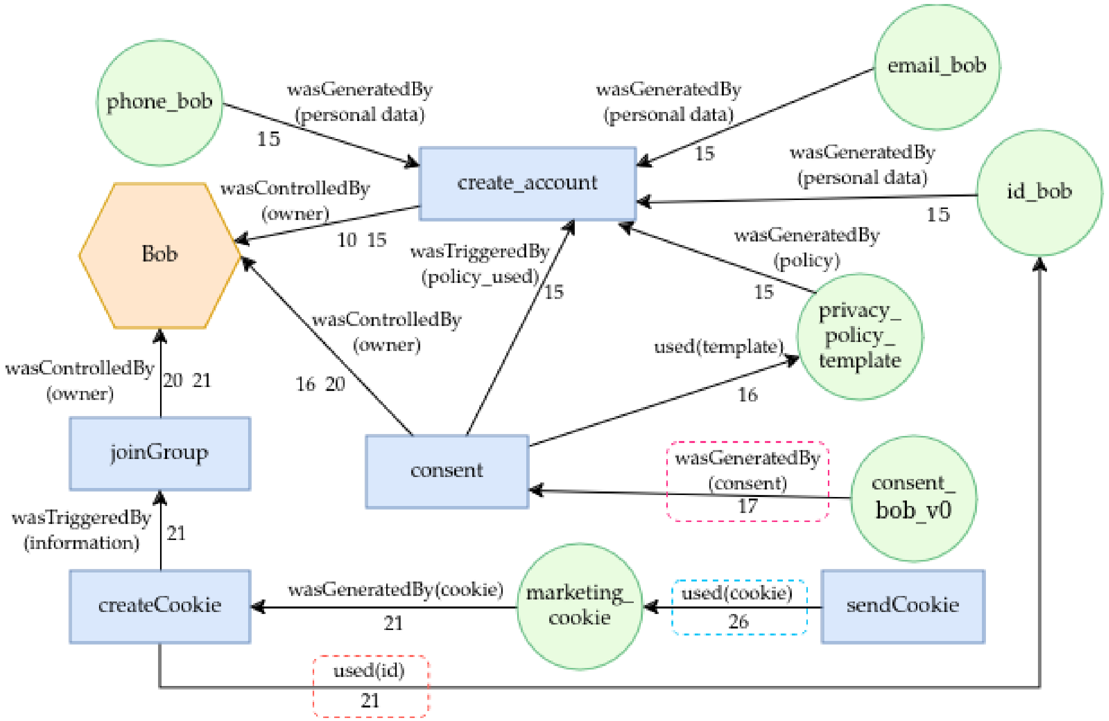
- Prolog predicate to verify consent compliance

```
consent(DP, PU, T) : −
    wasControlledBy(P1, S, ”owner”, TB, TE),
    wasGeneratedBy(C, P1, ”consent”, T), isPurpose(PU, DP, C)
```

```
predicate(parameters) :-
        ( verify parameters,
                ( verify compliance;
                (\+ verify compliance, display non-compliant data) ) );
        (\+ verify parameters, display no parameters).
```

- Verification:
  - Consent compliance for Bob personal data processing
  - Bob has given consent for ***analysis*** purposes only (represented by consent_bob_v0)
  - Only process using personal data:
    - createCookie
    - sendCookie

Prototype: an exemple

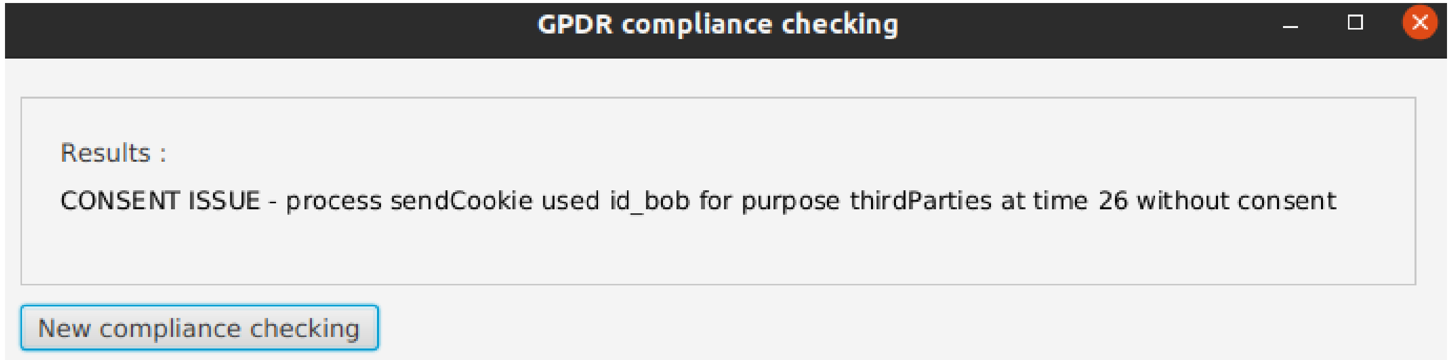


P =sendCookie, associated to a purpose ***PU=sendThirdParties***.

consent(*id_bob, **sendThirdParties**,T*)
→ don't exist

consent(*id_bob, analysis, 17*)

- The interface shows:



Results :

CONSENT ISSUE - process sendCookie used id_bob for purpose thirdParties at time 26 without consent

Future work

a) Provenance graph generator for more extensive testing

b) Improvements on the tool interface: including a visualization model

c) Extension to other regulations

Bibliography

1. [1]   D. Basin, S. Debois, and T. Hildebrandt. On purpose and by necessity: Compliance under the gdpr. In *Financial Cryptography and Data Security*, pp. 20–37. Springer Berlin Heidelberg, 2018.
2. [2] L. Moreau, et al. The Open Provenance Model core specification (v1.1). *Future Generation Computer Systems*, vol. 27, no. 6, pp. 743–756, June 2011.
3. [3] A. Tauqeer, A. Kurteva, T. Raj Chhetri, A. Ahmeti, and A. Fensel. Automated gdpr contract compliance verification using knowledge graphs. *Information*, vol. 13, no. 10, 2022.
4. [4] European Union. General data protection regulation, 2016. Accessed: 2024-08-23.