A blockchain-based framework for GDPR-compliant personal data processing

STELVIO CIMATO, CHIARA BRAGHIN AND MARCO DE SIMONE
Motivation

From 2018 GDPR strengthens the data rights of EU residents and harmonises data protection law across all member states

It has impact on any organisation holding personal data:
- more transparency to people about what data organisations collect about them,
- what those organisations use it for
- enabling people to prevent unnecessary data collection
- have full control over their personal data

It also increases the potential fines organisations face for misusing data

It requires (Art. 51) each member state to provide for one or more independent public authorities responsible for monitoring the application of the regulation, having access to all information necessary for the performance of their tasks.

Compliance to GDPR is then essential.
Sample scenario

Consider for example an online shopping service

- Throughout the sign-up process, the service collects consent and personal data such as name, address, email, and contact number.
- Users are requested to provide sensitive information for transactions about their bank account or credit card only when ordering products.
- All the collected personal data are recorded in a centralised database managed by the company.

As regards GDPR compliance:

- Personal data may not be directly and easily accessible to data subjects.
- Stored data may be not consistent with the consent or data given by the consumer, either by mistake (e.g., coding error) or on purpose.
- The changes (either of consent, or data) in the database might not be recorded in a log, thus not be traceable.
Blockchain as an authorization tool

Decentralising data storage helps:
◦ to record each interaction between the data subject and the service provider,
◦ bringing personal data processing to a level of privacy and security that prioritises data subjects and shared transparency,

Smart contracts can be used to encode GDPR legal requirements
◦ they are enforced automatically.
◦ becomes an access control manager that does not require a trusted third party
◦ blockchain can act as a tamper-proof ledger to record digital interactions
Framework for GDPR Compliance

A general framework that can be deployed by any organization for GDPR-compliant data processing.

- combining blockchain and off-blockchain storage to construct a personal data management platform
- A smart contract works as an intermediate layer/interface/component monitoring and recording each interaction between the user, the organisation and data.
- In particular, it will ensure that data will be modifiable only by the subject.

The subject must have full control of the data entered during registration and the authorizations granted.

The actions performed on data and authorizations (entering, modifying, deleting) must be traceable

The supervisory authority, if requested, must be able to access the data and be able to carry out the required checks.
Architecture of the framework
SMART CONTRACT

Contains all data structures required for storing authorizations

For each treatment, it stores an identified associated to the data treatment

Only those who are entitled to it can change the permissions granted
Java API

A Java library has been implemented and included in the prototype in order to facilitate the deployment of systems based on our framework.

The library offers APIs to the functions of GDPRContractActions smart contract, thus providing an abstraction from Ethereum.

By using the library, developers can implement GDPR-compliant client and server applications since by construction they meet the restrictions imposed by the GDPR and satisfied by the contract.
Use cases
Registration

- Interested
  - Inserimento dati nel form di registrazione
  - Pagina di conferma e indirizzo dello smart contract

- Servizio Web
  - Richiesta di inserimento di un nuovo trattamento
  - Conferma dell’operazione

- ContractLib
  - Esecuzione transazione per l’inserimento di un nuovo trattamento
  - Esito della transazione

- Smart Contract
  - Inserimento dati nella Blockchain
  - Risposta del database

- Database del titolare
  - Query di inserimento dei dati nel database
  - Salvataggio dei dati
Updating authorizations
Conclusions

The newly proposed system therefore represents a complete environment capable of integrating the smart contract with a corporate service.

Thank to the use of the proposed library,

- the developers can realise client and server applications for the needs of the company and customers
- smart contract can be adapted
- meet the restrictions imposed by the GDPR.

Future works:

- Compatibility and integration with already developed services
- Simplified interaction
- More detailed analysis (security and cost analysis, formal/semi-formal)