BLOCKCHAIN FOR GDPR COMPLIANCE

Whitepaper

Abstract

[The General Data Protection Regulation(GDPR) regulates the export of personal data outside the EU. The regulation has provisions for individual control over one's own data that includes many rights to the individual to manage personal data -access, consent, removal, portability and minimization. It becomes enforceable from 25 May 2018 after a two-year transition period. Enter Blockchain, a distributed ledger technology creating decentralized digital identity networks that provide publicly auditable and valid data. For a self-sovereign identity, these methods provide a neutral, trusted and secure mechanism of managing data as per GDPR requirements]

RapidQube Digital Solutions Pvt. Ltd.,
info@rapidqube.com

GDPR Compliance Platform

Introduction

The **General Data Protection Regulation**(**GDPR**) is a regulation by which the European Parliament, the Council of the European Union and the European Commission strengthened and unified data protection "rules" for all individuals within the European Union (EU.) The regulation was adopted on 27 April 2016 and becomes enforceable from 25 May 2018.

RapidQube focused on those Articles where we felt we could apply blockchain, digital signature and smart contract solutions to address the requirements presented.

RIGHT TO ACCESS

Article 15 of the regulation stipulates that an individual has the right to understand who has access to their personal data, what data has been made available and how that data is being used or processed ("tell me who, what, when.") In addition, the individual must be able to obtain, on demand and with no charge, a copy of the digital information undergoing processing.

In blockchain, the entire process is tracked, timestamped, and built into an immutable record that builds the block. This data can be retrieved by the data subject or individual at any point of time.

RIGHT TO CONSENT

While not new in the world of compliance, this regulation stipulates, specifically in Article 7, that an individual must consent to data being used and, moreover, has the right to rescind that consent at any time.

By design, blockchain leverages consensus algorithms that necessitate approval from the data subject or individual ("ask me.") The consent is sought for each and every access request. The individual or data subject can revoke the requestors or controllers access whenever needed.

RIGHT TO BE FORGOTTEN

In Article 17 the right to be forgotten means that an individual has the right to ensure that the data being used in and out of the processes be managed. There should be stewardship of that data.

Blockchain holds the key to storing personal data. In case of a delete request ("forget me") by an individual, the personal data which is held in any system external to the distributed ledger or blockchain is permanently deleted and the “key” that enabled that connection initially to the blockchain is also permanently deleted.

RIGHT TO PORTABILITY

Article 20, the right to portability defines how an individual should be able to obtain, move and provide access to their digital data as they see fit ("come with me.”)

In the blockchain or distributed ledger, access to Personally Identifiable Information (PII) is time bound and secured by the use of an encryption technology, called "hashing." For blockchain, this level of encryption is the "game changer.”

RIGHT TO DATA MINIMIZATION

In Article 5, only the minimum personal data which is absolutely necessary for any specific purpose in a processing request will be used (“use the least of me.”) Think less, not more. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility.

A data subject or individual can share whatever subsets of personal data are needed. In blockchain, the use of a “Proof-carrying code” technique should minimize the need to expose any data contained in the validation process itself.

RIGHT TO RECTIFICATION

In Article 16, the data subject shall have the right to obtain from the controller, without undue delay, the rectification of inaccurate personal data concerning him or her (“use what’s correct about me.”) Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

The blockchain or distributed ledger facilitates update of data whenever required by a mutual consensus between the data subject and controller and that data gets shared to other participating entities in the network.

BLOCKCHAIN SOLUTIONS

MANAGING PII-THE BASIS FOR GDPR COMPLIANCE

We can demonstrate that GDPR Compliance has been achieved by recording the PII transactional events on Blockchain without the need of any additional components that may be required in a traditional model.

- The features of Blockchain data: provenance, immutability, distribution, and real-time synchronization of PII across collaborators along with record of occurrence time stamp prevents any kind of fraudulent activity on personally identifiable information (PII).
- The built-in components of blockchain such as encryption, anonymization and pseudonymization, data access management protect PII information helps in rapid implementation of a compliance platform to meet the GDPR requirements.

Articles	Description	Blockchain Design Element \ Attribute
RIGHT TO ACCESS	emphasizing transparency for data subjects	Distributed Ledger & Digital Signatures

RIGHT TO CONSENT	having a lawful and legitimate purpose for processing the information in the first place	Smart Contracts
RIGHT TO DATA MINIMIZATION	ensuring data is adequate, relevant and limited, and organizations are capturing the minimum amount of data needed to fulfil the specified purpose	Smart Contracts
RIGHT TO PORTABILITY	protecting the integrity and privacy of data by making sure it is secure, which extends to IT systems, paper records, and physical security discouraging unnecessary data redundancy and replication	Channels / Streams - Anonymising and Pseudonymising the data
RIGHT TO BE FORGOTTEN	demonstrating compliance when there is a need to removal of data	Encryption & Hashing
RIGHT TO RECTIFICATION	requiring data controllers to make sure information remains accurate, valid, and fit for purpose	Smart Contracts

Scenario: Compliance reporting on Employee data– Blockchain approach
The contact details of employee can live in the legacy systems very much similar to that in the traditional approach. But the hash of the data, timestamp and the sensitive PII information are recorded in a common BUS i.e., Blockchain based GDPR Compliance Platform.
All other applications including HRMS in the Organization rely upon the Platforms API's to associate the Employee data with the PII information stored in the BUS.

Being on Blockchain, without even enabling any additional services, this recorded hash is immutable and will serve as evidence to address any tampering over the data recoded in the legacy system.

Using digital signatures, the PII information is protected from any unintended or illegitimate access, thereby making the system more secure from data hack.

This approach of pseudonymizing the data and auditing any changes to the contact details through Blockchain is a more reliable solution for demonstrating Compliance of Employee data to GDPR requirements.

Blockchain GDPR Compliance Platform Architecture

The below diagram represents sharing of PII data through blockchain among partner organizations.

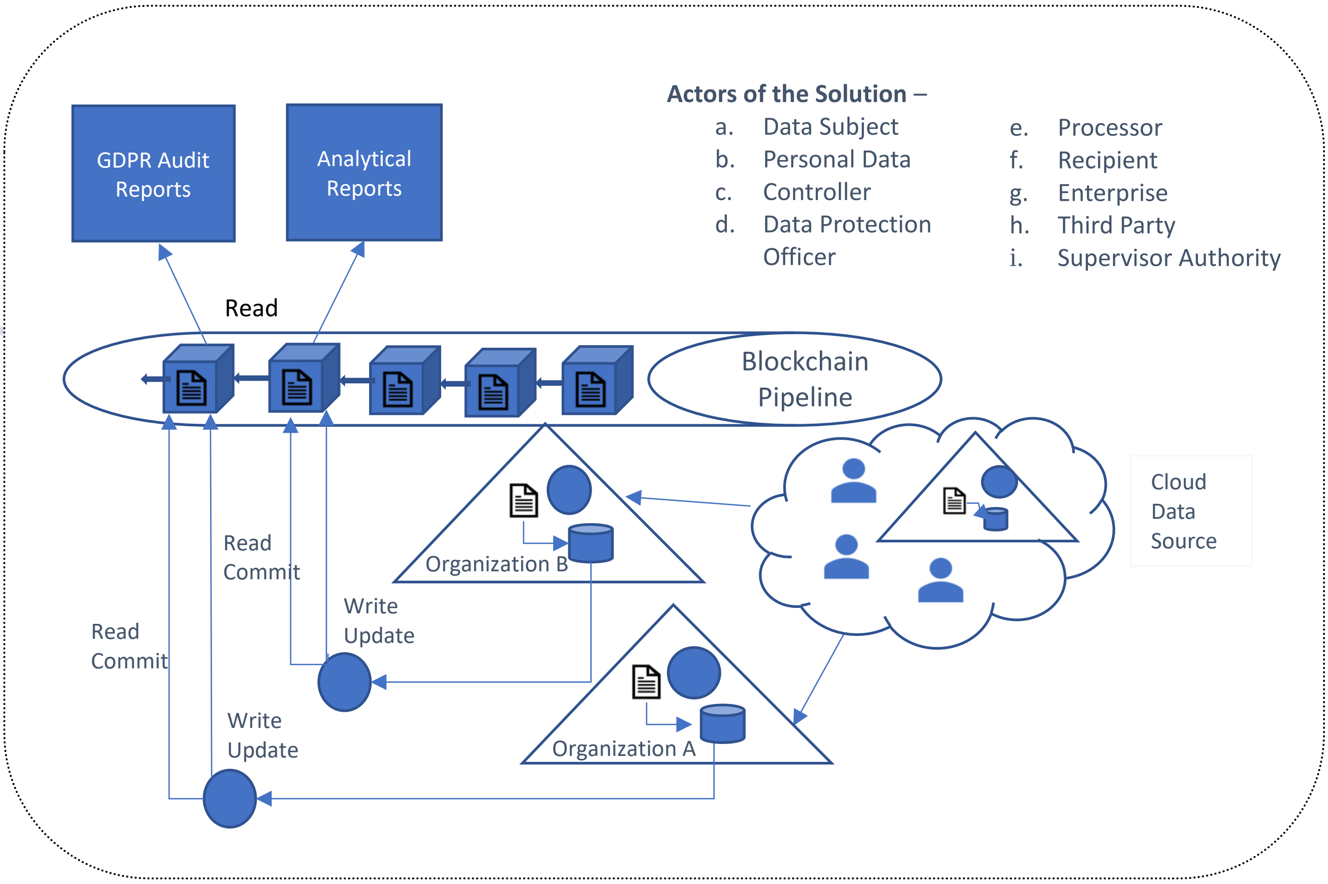
Organization: Each organization stores PI information in its own data storage, but when the data is modified, the platform generates a new hash and corresponding time stamp gets committed to the blockchain.

Cloud data source: Represents the various source of information flow that comes from multiple organization systems, naming few sources of information such as mobile applications, SAP systems, external applications, cloud systems, mainframe systems, payment gateways, etc.

Blockchain Pipeline: Represents the ever-growing set of blockchain. Blockchain pipeline will get connected to different organizations for read and commit new data in a blockchain which will get stored either as real data or as a hash which is reference to real data.

GDPR Audit reports: Represents the reports. Audit reports is secured and permissioned data. These reports can be used by data protection officer for auditing.

GDPR Analytical Engine: Helps us in continuously monitor events, gather insights and it will also help us in capturing the alerts if any data compromise or breach is triggered.



Actors of the Solution –

a. Data Subject
b. Personal Data
c. Controller
d. Data Protection Officer
e. Processor
f. Recipient
g. Enterprise
h. Third Party
i. Supervisor Authority

Component & Data Layers

The below lists the data layers supporting the GDPR platform based on the architecture described above –

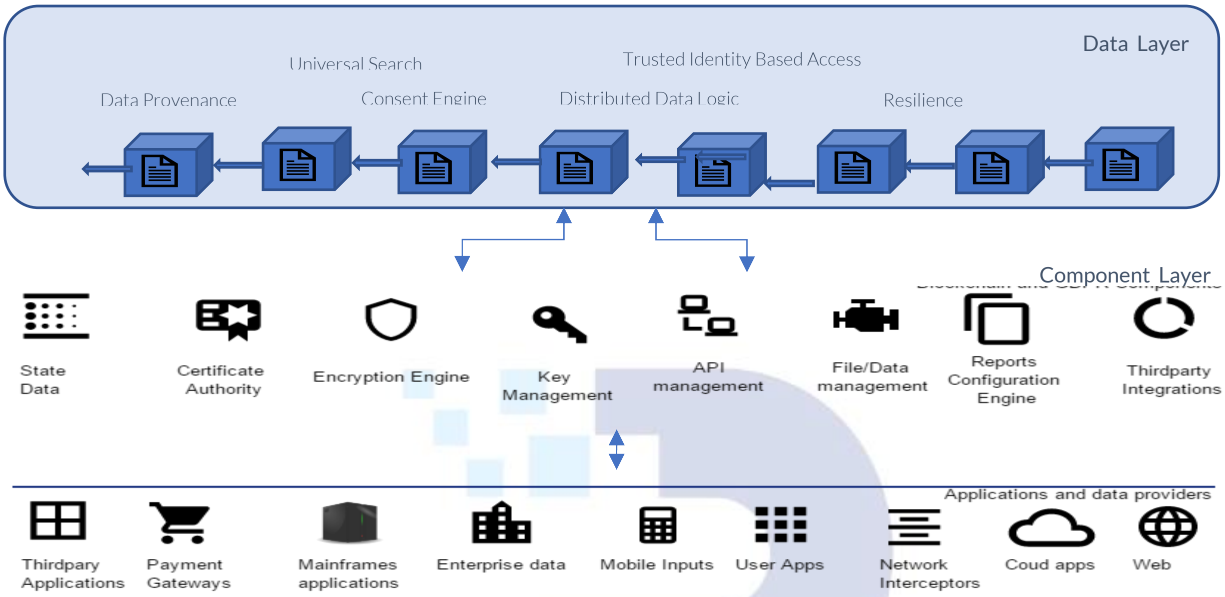


Illustration of functionality of Architecture components in a HIE scenario

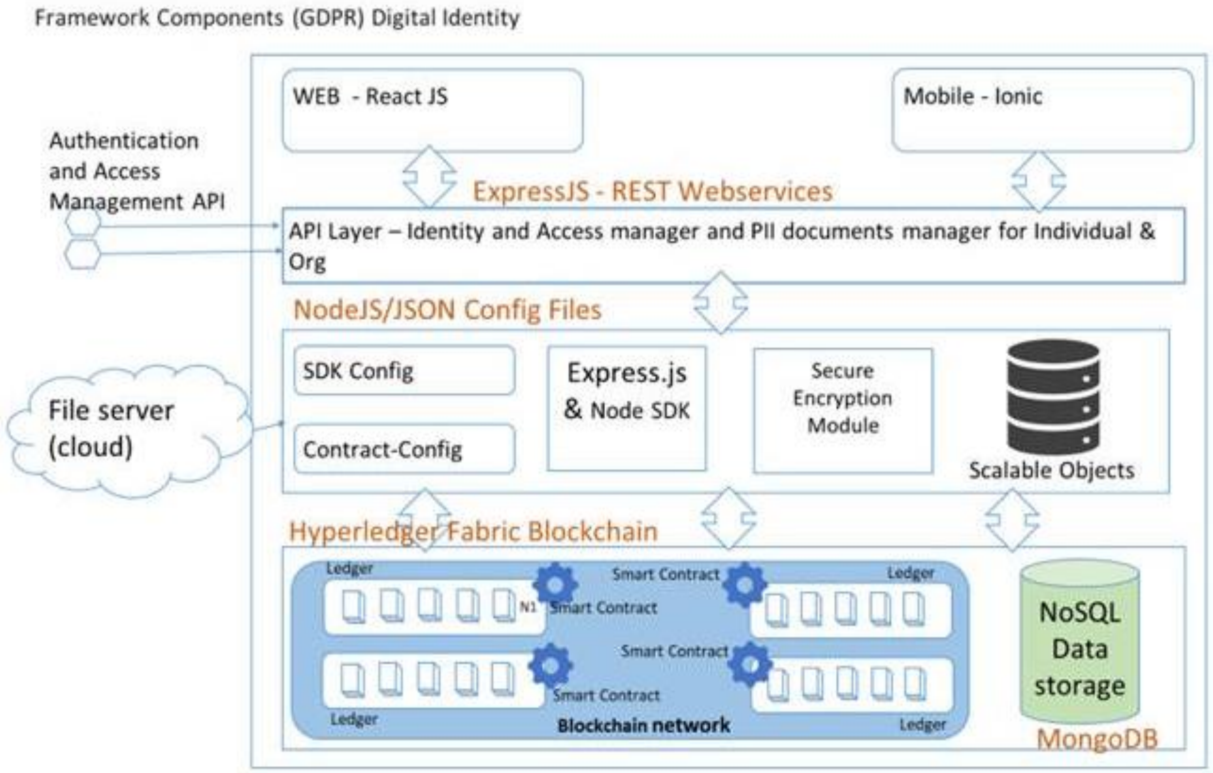
Payer shares the current health status, as reported by a claimant, to a third-party Health Information provider for verifying the sanctity of data submitted. The input to the Information provider includes a pseudo-identity attribute for mapping the outcome of verification with the corresponding claimant record at the Payers end. This attribute helps Payer to avoid revealing the actual identity of the claimant to the Information provider. But, as there are possibilities of exposing or compromising this identity of the claimant at both the ends, this PII involved in this information share is subject to GDPR.

The State Data component of the architecture records the state of the current shared health status information in the form of a hash generated by the Encryption engine along with the details about the receiving end as in the Certification Authority to the immutable Distributed ledger. Similarly, on any subsequent share with a different entity maybe for a re-verification, the details of the receiving entity as in the Certification Authority is appended by the State Data component to the hash of the information share.

On completion of the process, the Payer requests deletion of claimant data, if held in any form from the subscribing entities. Using the receiving end details associated with the hash of the share in the Distributed ledger, the Smart Contract notifies all subscribing entities to provide confirmation on removal of the corresponding data. An alert is also triggered by Smart Contract through API to all participating entities at regular intervals to prevent any data breaches. The immutable Distributed ledger tracks the end to end process along with the time of event occurrences as required for Audit and reports at scheduled intervals through the Reporting engine.

Implementation Architecture

The below lists the tools & technologies used by GDPR Platform based on the architecture illustrated above -



Mapping of GDPR Articles to Blockchain Design

1. RIGHT TO ACCESS: *"Who accesses personal data, what data has been made available and how the data is being processed"*
   Data Subject can access its complete PII data along with timestamp, receiver details, and other processing metadata. All these are stored in the ledger as immutable records and can be retrieved only by data subject at any point in time.

2. RIGHT TO CONSENT: "*Must consent to data being used and, moreover, has the right to rescind that consent at any time."*
   The data subject's PII information is recorded only after validating its consent through smart contracts and various other algorithms. Data subject can at any point of time remove the keys of recipient which would revoke the recipient's access to the data subjects PII data.

3. RIGHT TO DATA MINIMIZATION: "*Mandated to use only personal data which are necessary for each specific purpose of the processing are processed*."
   Proof-Carrying code technique evaluates the personal data and provides only the result that to meet the exact requirement of Recipient.

4. RIGHT TO PORTABILITY: “*Receive personal data provided to a controller in a digital format and may transmit that data as desired.* “
   The data subject shares Personally Identifiable Information (PII) with controller for a definite period and Controller wouldn’t be able to share personal data of data subject. The share can be initiated only by the data subject.

5. RIGHT TO BE FORGOTTEN: “*Demand that data controller erases any or all data held about an individual by that controller.”*
   The GDPR platform stores PII data of the data subject in a Document DB and the key/hash of data in blockchain. In case of delete request, the link or reference to the data stored in the Document DB that is outside of blockchain is removed thereby the identifying key in the ledger loses its reference to PII data permanently.

6. RIGHT TO BE RECTIFICATION: “*Demand that data controller provides corrections to any or all data in a timely fashion.”*
   The GDPR platform provides the ability to update and correct PII data between the data subject and controller across all the approved entities in the network.