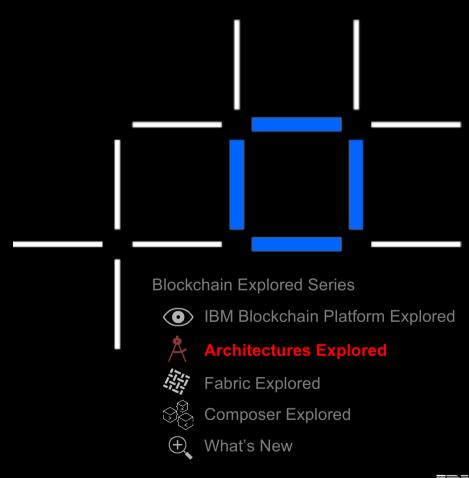
Architectures Explored - GDPR

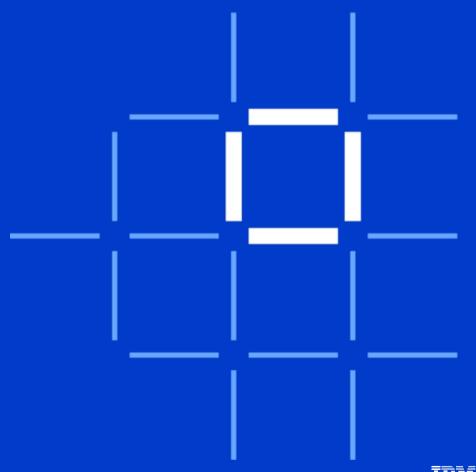
Best practices for GDPR-compliant blockchains



V1.0, 8 June 2018



Summary of GDPR



IBM **Blockchain**

IBM.

General Data Protection Regulation (GDPR) – Overview

- GDPR became law on 25th May 2018
- Applies to organisations operating within the EU, also applies to organisations outside the EU who offer goods/services to EU individuals
- Fines of €20m or 4% of global revenues

Organisations can be either/both

Data Controller

Determines the purpose and means by which personal data is processed

Contracts with processor must be **GDPR** compliant

Data Processor

Processes data on behalf of data controller

Legal Contract specifies GDPR duties to the controller

The processor must provide sufficient guarantees they will implement measures to meet GDPR.

Data

Personal Data

Any information relating to an identified or identifiable natural person

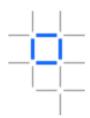
- **Employee** or **Customer**
- New rights include:
- **Information** about processing
- Obtain access to PD
- Request corrections to PD
- Data be erased

Subject

- Object to being used for marketing
- **Restriction** of processing
- **Data portability**
- Automated processing of PD



General Data Protection Regulation (GDPR) – Links



- Rights for citizens
 - https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/my-rights/what-are-my-rights_en
- What is Personal Data?
 - https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en
 - Examples: Names, Address, Email, ID Card number, Location Data, IP Address, Cookie ID,
 Advertising ID
 - https://ico.org.uk/media/for-organisations/documents/1554/determining-what-is-personal-data.pdf
- What is a data controller or processor?
 - https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_en
- Official Journal
 - http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN



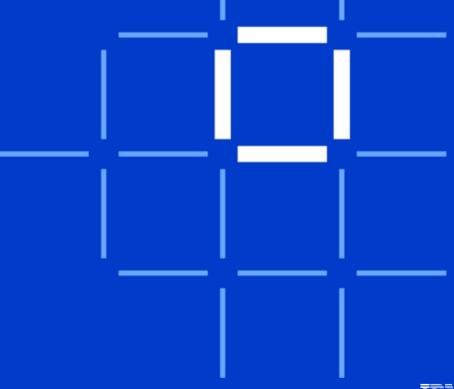
Further Reading



- UK Information Commissioner's Office (ICO) Data Protection Act (DPA) document that helps determine if data is considered Personal Data. DPA is being superseded by GDPR:
 - https://ico.org.uk/media/for-organisations/documents/1554/determining-what-is-personal-data.pdf
 - DPA and GDPR
 - https://www.itgovernance.co.uk/data-protection
 - Anonymisation
 - https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf
- NHS in the UK document on Anonymisation and Pseudonymisation Standard:
 - https://www.nhsbsa.nhs.uk/sites/default/files/2018 03/NHSBSA%20Anonymisation%20and%20Pseudonymisation%20Standard.pdf



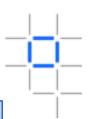
"Right to Erasure" and Blockchain



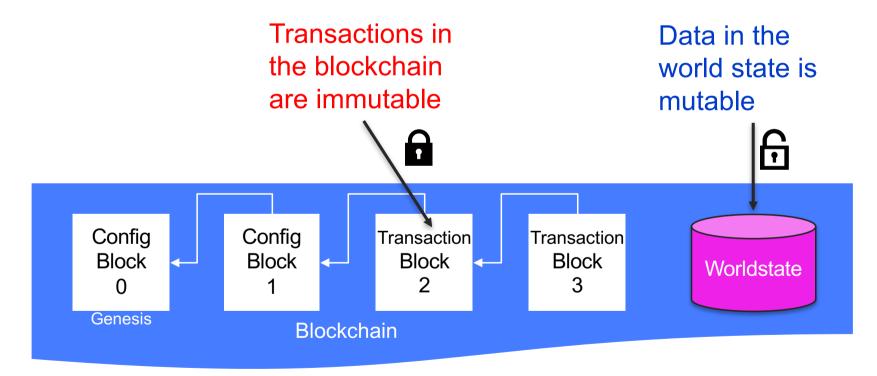
IBM **Blockchain**

IEM

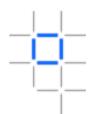
The "Right to Erasure" and blockchain



Enables an individual to request the deletion or removal of their personal data

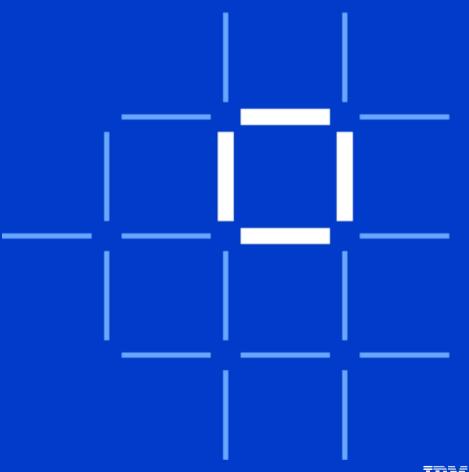


Further Reading



- UK Information Commissioner's Office (ICO) "Right to Erasure" guidance:
 - https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure

Hyperledger Fabric Block



IBM **Blockchain**

IDM.

Summary of a Hyperledger Fabric Block

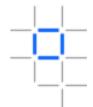


• Fields highlighted in red could potentially contain Personal Data recorded on the blockchain.

1	Header			Number	Previous hash	n (merkel root)	Data hash (merkel root)
Block	Block Data (repeated per transaction)	Signature		Client signature of transaction payload			
		Payload	Header	Channel Header (timestamp, tx_id, type,)		Signature Header (client certificate)	
			Data	Client certificate		Mspld	
				Proposal payload		Proposal hash	
				Array of keys read (key and version of value)			
				Array of keys written (key/value and delete flag)			
				Array of range_queries (start/end key and list)			
				Events (chaincode_id, tx_id, name, payload)			
				Chaincode response (status, message, payload)			
				Chaincode ID (path, name, version)			
				Array of endorsers (mspid, certificate, signature)			
- 1	Block Metadata			Array of orderers (mspid, certificate, signature)			
Ţ				Array of transaction valid flags			
ماد	←	Index	\longrightarrow	Data			



Block Fields and Personal Data



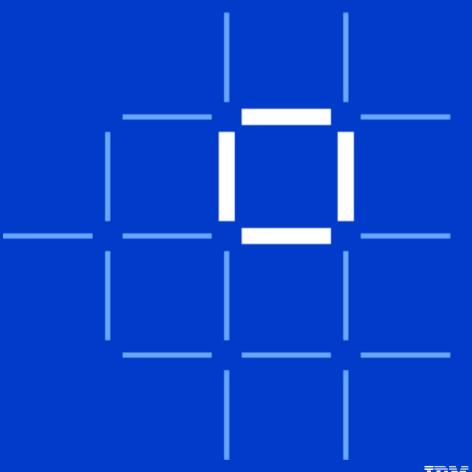
This slide describes the potential areas that Personal Data could be included in the block:

- Proposal payload: These are the transaction input arguments.
- Client certificate: If the client certificate is individual to a Data Subject then it could be considered PD.
- **Key:** The key written to or read from the world state. If PD is used in the key name then it will be included here.
- Value: The value of any keys written to the world state. If PD is used in the key value then it will be included here.
- Events: Events emitted from chaincode could include PD.
- Chaincode response: Any response from invoking the chaincode could include PD.

It is assumed that endorser and orderer certificates are issued to an organization and do not include Personal Data.

Remember that Fabric configuration blocks also contain certificates!

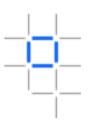
Solution



IBM Blockchain

IDM.

Solution – Store data off-chain



What

The only approach is to store Personal Data in an off-chain mutable data storage

How

 Store only proofs of the PD on the blockchain with hashes linking to PD (all hashes must be salted)

Config

Block

0

Genesis

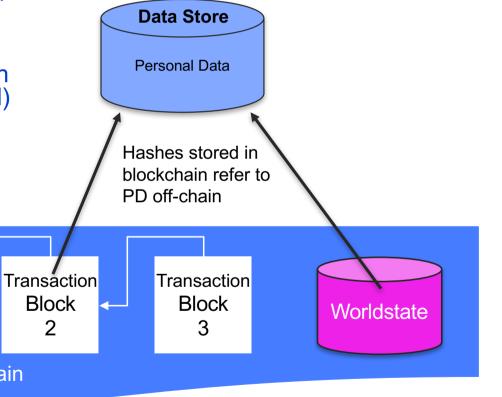
Config

Block

Blockchain

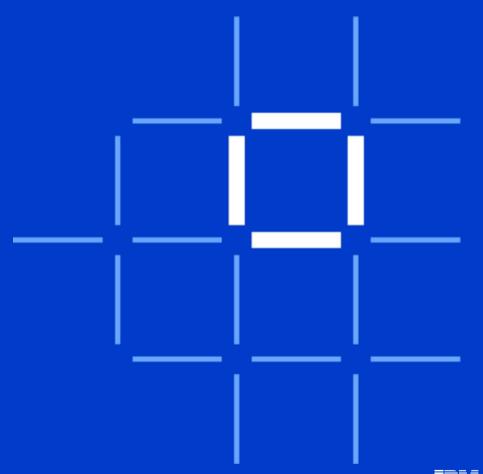
Why

PD can be deleted at any point from the data store(s)



Non-Compliant Solutions

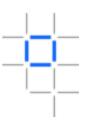
These are non-GDPR compliant



IBM **Blockchain**

IEM

Store Personal Data in Private State (SideDB)



What

 Send Personal Data in transient part of blockchain transaction, save PD in private state and hashes on the blockchain

How

PD is sent in the transient data field to the Smart Contract (FAB 2450), data stored in private state, hashes are stored on the channel and writeset is stored in the private writeset storage (FAB 1151). Requires Fabric 1.1(*).

Why not compliant

 FAB 1151 stores the private data writeset in storage similar to a blockchain. This private writeset storage cannot be deleted (other than a blockToLive policy on the collection) and therefore a request to erase PD cannot be processed.

Confia

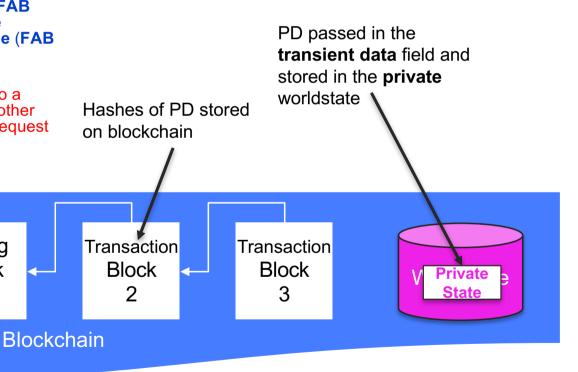
Block

0

Genesis

Confia

Block



Encrypt data

- What
- Encrypt Personal Data before being stored on blockchain
- How
- Public/Private Keys must be secured in a mutable data store

Config

Block

0

Genesis

Config

Block

Blockchain

- Why not compliant
- Unproven for compliance with GDPR

