Transforming Personal Data Transactions with Auditable, Privacy-Preserving Data Exchange Agreements

Fostering Transparency and Trust in Digital Wallet Ecosystems

Lal Chandran, Lotta Lundin and George Padayatti
iGrant.io, Stockholm, Sweden

lal@igrant.io, lotta@igrant.io, george@igrant.io

***Abstract* - This paper proposes a comprehensive data exchange framework that addresses key digitalisation challenges and integrates regulatory compliance, usability, auditability, and transparency. The human-centric approach enables auditable data sharing, enhances security and privacy, and applies to centralised and decentralised systems, as evaluated in a digital wallet-based dataspace ecosystem.**

Keywords— auditability, data agreements, digital wallets, privacy, regulatory compliance, transparency

I. INTRODUCTION

In the age of digital transformation, data access has become crucial for individuals and organisations. However, ensuring data privacy, regulatory compliance, transparency, and auditability has become a major challenge. The General Data Protection Regulation (GDPR) [1] and other emerging regulations have attempted to address some of these challenges, but effectively implementing these measures while mobilising data remains an issue [2][3]. Some key challenges are as follows:

Fear of non-compliance: The impact of GDPR on different business models and organisations has been explored in several studies [1][2], highlighting the challenges and opportunities in complying with the regulation.

The legal penalties imposed by GDPR and similar regulations have led organisations to adopt cautious approaches to digitalisation. This is particularly evident among small and medium-sized enterprises (SMEs) and government entities. The crucial challenge for these organisations is continuing their digitalisation efforts while providing valuable services to their customers, given the potential risk of non-compliance with GDPR and related regulations. The impact of GDPR on different business models and organisations has been explored in several studies [1][2], highlighting the challenges and opportunities in complying with the regulation. Lindgren [4], for example, discusses how different business models and businesses are impacted by GDPR, highlighting the need for organisations to balance compliance with digital innovation.

The difficulty of obtaining meaningful consents and agreements: Obtaining consent from individuals to use their personal data is a complex issue, often made difficult by long and complex privacy policies and terms of service agreements. This can leave individuals unsure about what they agree to and how their data will be used, with no auditable log of their agreements [3]. The consent fatigue and the non-transparent manner in which they are obtained result in individuals saying no to sharing their data unilaterally. This can lead to a lose-lose situation, where organisations cannot leverage data to provide advanced personalised services, and individuals miss out on the benefits of such services.

Lack of trust and transparency deficit: Hinds et al. [2] found that the Cambridge Analytica scandal resulted in a significant lack of trust and transparency towards organisations collecting and using personal data. The scandal caused individuals to become more aware of the extent of personal data being collected, how it is being used, and who has access to it. This increased awareness led to concerns about data breaches, identity theft, and the misuse of personal information.

Furthermore, these studies found that individuals are often unaware of how their data is being collected or used due to lengthy and complicated privacy policies and terms of service agreements. This lack of transparency and the complexity of agreements makes it difficult for individuals to give meaningful consent. As a result, individuals are more likely to say no to sharing their data unilaterally due to the perceived lack of transparency and trustworthiness of organisations collecting personal data.

To address the identified challenges, this paper proposes a practical approach incorporating risk-based compliance to regulations, a human-centric and usable approach to obtaining consents or agreements. Furthermore, it employs cryptographic mechanisms to ensure transparency and auditability for every data exchange transaction through a data exchange protocol. This significantly differs from many existing proposals in that it provides a complete framework that can be applied across the industry sectors. The protocol builds upon the concept of data disclosure agreements (DDAs). A DDA is a legally binding contract governing personal data sharing between individuals and organisations. DDAs provide a framework for the terms of data sharing between organisations, including the purpose, scope, and duration of the sharing and the security and privacy measures that must be implemented. The proposed protocol enhances the framework by incorporating digital rights management in the data agreements, enabling individuals to control their data and facilitate secure and responsible data exchange.

The reference system for the protocol is a digital wallet-based decentralised dataspace ecosystem. Digital wallets are secure digital storage and exchange solutions that allow individuals to store and manage their personal data while maintaining control over who has access to what data and for what purpose. By incorporating the proposed protocol into digital wallets, individuals can control the data they share, and organisations can ensure compliance with regulatory requirements. Overall, the proposed protocol aims to provide a secure, auditable and transparent solution for data exchange while prioritising the privacy and rights of individuals.

This paper addresses the problem of privacy-preserving and data regulatory data exchange and proposes an auditable framework with a practical implementation using digital wallets. The framework is applicable to a wide range of Web 2.0 and Web 3.0 digital service scenarios. It is divided into various sections - The background section provides an overview of key challenges in the use of personal data in the digital economy. The methodology chapter elaborates on key concepts related to data exchange used in the proposed framework. Chapter IV specifies how the framework is implemented; Chapter V elaborates on selected cases where the framework is applied and evaluated. Chapter VI provides related work in the area with conclusions in Chapter VII.

II. BACKGROUND

A. GDPR and Emerging Data Regulations

GDPR, or the General Data Protection Regulation [1], is a set of regulations introduced in 2018 to govern how organisations in the European Union (EU) handle personal data. The GDPR is one of the world's most comprehensive data privacy laws. It applies to any organisation that collects, processes, or stores the personal data of individuals within the EU, regardless of where the organisation is based.

The GDPR aims to give individuals more control over their personal data and ensures that organisations responsibly handle it. The regulation requires organisations to obtain clear and explicit consent from individuals before collecting or processing their personal data and to provide individuals with access to their data upon request.

In addition to the GDPR, other data regulations are emerging globally, such as the California Consumer Privacy Act (CCPA), Canadian Consumer Privacy Protection Act (CPPA) and the Brazilian General Data Protection Law (LGPD). These regulations further emphasise the need for organisations to protect individuals' personal data and to ensure transparency and accountability in data processing.

B. Data Misuse

Digital transformation has led to the explosion of data collection and exchange, making it a valuable asset for businesses across industries. With increased data collected and processed, the risk of misuse has also increased [2]. This has prompted governments worldwide to enact stricter regulations to protect individuals' privacy and digital rights [5]. The impact of data misuse is not limited to the loss of privacy and the individual harm caused by it. It also has far-reaching consequences for businesses and society, resulting in a significant trust deficit. Consumers are increasingly becoming aware of the value of their personal data and are losing trust in businesses that fail to protect it or use it for other purposes than agreed. This trust deficit makes it difficult for businesses to build long-term customer relationships, hampering their ability to innovate and grow. In addition, the reputational damage resulting from data breaches can be severe, leading to significant financial and legal consequences for businesses. Therefore, businesses must adopt measures that safeguard personal data and build customer trust.

C. **Transparency Missing**

The need for transparency in personal data processing in organisations is crucial for ensuring individuals' right to self-determination, privacy, and a democratic society [6]. Many companies collect, store and share data, often without the knowledge of the individuals concerned. Many have been criticised for lacking data collection, storage and sharing transparency. This lack of transparency is particularly prevalent in industries that rely heavily on data, such as social media and advertising. For example, Facebook, TikTok etc., has been embroiled in several scandals related to data privacy and has been accused of not being transparent enough about how it collects and uses data.

Other industries, such as healthcare and finance, face challenges in ensuring transparency. In healthcare, for example, patients may not know what data is being collected about them and who has access to it. This lack of transparency can lead to concerns about privacy and security. In healthcare, for example, patients may not know what data is being collected about them and who has access to it. This lack of transparency can lead to distrust, as people may not know what information is being collected about them or how it is being used. Hence, companies and industries must be transparent about how they collect, store, and use data to build trust with customers and the wider public and to ensure that individuals continue to say yes to sharing their data.

The various criteria for enabling transparency at scale in the processing of personal data can be summarised [7] as below:

- *Availability*: individuals should have access to their personal data and be able to verify its accuracy and completeness.

- *Understandability*: individuals should be able to understand how their personal data is processed, including the purposes for which it is used.

- *Timeliness*: individuals should be informed about processing their personal data on time, particularly in cases where data is processed without their consent.

- *Granularity*: Individuals should be able to choose which types of data they want to share and with whom.

- *Traceability*: individuals should be able to track the processing of their personal data and identify any entities that may have accessed or used their data.

- *Context-awareness*: individuals should be informed about the context in which their personal data is processed, including any relevant legal or ethical considerations.

For example, the European Legal Data Protection Framework reinforces the above criteria by granting individuals information, access and control rights and enforcing transparency and intervenability [1]. These criteria have been used as the backbone to develop the proposed methodology in this paper.

D. Digital Identity Wallets and Verifiable Credentials

Digital Identity Wallets and Verifiable Credentials [8] technologies enable individuals to maintain control over their personal data and share it securely and selectively with other parties while providing enhanced privacy, security, and usability. Digital Identity Wallets are software applications that allow individuals to store and manage their personal information in a secure and decentralised manner. They enable users to manage their identities across multiple online platforms and services while providing high privacy and control. By storing personal information on a user's device rather than on a centralised server, Digital Identity Wallets eliminate the need for users to trust third-party service providers with their sensitive personal information.

Verifiable Credentials are a key component of Digital Identity Wallets, including EU Digital Identity (EUDI) Wallets [9]. They are digital representations of real-world credentials such as driver's licences, passports, and academic degrees. Verifiable Credentials enable individuals to prove their identity and qualifications without sharing their sensitive personal information with third parties. They are cryptographically secured, tamper-proof, and can be verified instantly by anyone with the appropriate access rights.

Digital Wallets (including EUDI Wallets) and Verifiable Credentials promise to enhance privacy, security, and usability in the digital world. They enable individuals to take control of their digital identities and personal information while also providing a more transparent and trustworthy ecosystem for data sharing and exchange.

III. METHODOLOGY

E. The Data Exchange Agreement Landscape

A typical data exchange ecosystem requires several agreements to validate the data exchanges legally. Based on the roles and the relationship that exists between the parties in the data exchange ecosystem, these agreements can be classified into four categories:

a) An individual and an organisation
b) Two organisations
c) An organisation and its supplier,
d) Two individuals

The data exchange agreement (DEXA) landscape, based on the above roles, is illustrated below.

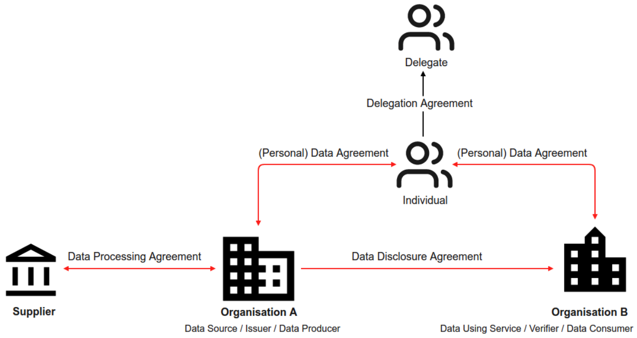

Delegate
Delegation Agreement
(Personal) Data Agreement
(Personal) Data Agreement
Individual
Data Processing Agreement
Data Disclosure Agreement
Supplier
Organisation A
Data Source / Issuer / Data Producer
Organisation B
Data Using Service / Verifier / Data Consumer

Fig. 1. The Data Exchange Agreement Landscape

a) Data Agreement (DA) or Personal Data Agreement

A personal data agreement, simply called a data agreement, is an agreement between an organisation and an individual for using and processing personal data. It records the conditions for an organisation to process personal data in accordance with data protection regulations. An organisation can be a DS or a DUS. A DA can have any lawful bases as outlined by the relevant data protection regulation (such as the GDPR) and can be used, for example, for third-party data exchange. Regulations could be laws, norms (such as the MyData principles) or architectures inspired by Lessig's modalities of regulation [10].

The key characteristics of a DA are as follows:

- is associated with any personal data usage, including data exchange towards any DUS

- it can rely on an individual's consent or other lawful bases such as contract, legal obligation, vital interests, public task and legitimate interests by outlining the purpose for which personal data is to be processed

- is tied to a data protection impact assessment (DPIA) that further strengthens legal compliance for the organisation.

iGrant.io automates the conversion of the results of a DPIA to a machine-readable DA

- is standardised (ISO/IEC DTS 27560) under technical committee ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection WG5: 27560 [27]

b) Data Disclosure Agreement (DDA)

A Data Disclosure Agreement (DDA) exists between two organisations where one organisation is a DS (Data Source) and the other as a DUS (Data Using Service). The DDA captures how data is shared between the two organisations and each party's role and obligation as a data processor and controller. For any organisation involved in the data exchange, there is an associated DA that explains the purpose of processing personal data, what personal data is collected, what the data subject rights are, etc.

c) Data Processing Agreement (DPA)

The third form of an agreement exists between an organisation and its suppliers, as illustrated in Figure 1. Here, there is a relationship between Organisation A as a data controller and its supplier as a data processor or sub-processor. For a higher level of accountability between these organisations, a DPA is set up, which lays out what routines are required to be in place: for example, a data processor's obligations in case of a data breach or how the rights of the individual, such as access rights, are supported, among other policies and routines. An auditor should also be able to inspect the organisation and use the DPA as reference material during the inspection. As depicted in Figure 2, the DPA is connected to the individual at the top of the hierarchy via the data controller organisation.

d) Delegation Agreement

The delegation agreement is included to complete the data exchange ecosystem. A delegate may act on behalf of an individual in signing off any data exchange. There are several scenarios where delegation is necessary, for example, in the case of guardianship when an individual is incapable of signing off or in case an individual is given temporary rights to sign off on behalf of the individual, for example purchasing medicine at a pharmacy.

F. Actors involved in a Data Exchange Ecosystem

The key actors involved in the DA and DDA lifecycle are described below:

Data Source: the organisation that collects and stores personal data. They are also referred to as issuers or data producers.

Individual or the Data Subject: is the natural person who can manage their preferences, follow their data, and know who is consuming what, when and why. They are also referred to as holders.

Data Using Service: is the organisation processing personal data from one or more data sources to deliver a service.

Assessor: The individual who reviews the practices of an organisation (DS or DUS), conducts a DPIA and drafts data agreements and inter-company agreements for third parties

Auditor: The individual who may be called in to review the data agreements and ensure they are in place in case of data breaches or regular inspection handled

Data marketplace: in a dataspace is the platform where organisations (DUS) can discover the DS', and enter into a trust relationship. Here, the DS offers its data to potential DUS'.

The table below summarises the involvement of various actors in the DA and DDA lifecycle.

TABLE I. KEY ACTORS

Actors	**Data Exchange Agreement Workflow**	
	DA Lifecycle	***DDA Lifecycle***
Individual/ Data Subject	x	-
Data Source (DS)	x	x
Data Using Service (DUS)	x	x
Assessor	x	x
Auditor	x	x
Data Marketplace	-	x

G. The Data Exchange Agreement Workflow

An organisation wishing to use the DEXA workflow first performs a Data Protection Impact Assessment (DPIA) or similar. The result of a DPIA outlines the various data processing activities, the associated risks and mitigations. The DPIA report is important for demonstrating compliance with data protection regulations, such as the GDPR. The proposed process flow converts the DPIA outcome to machine-readable data agreements.

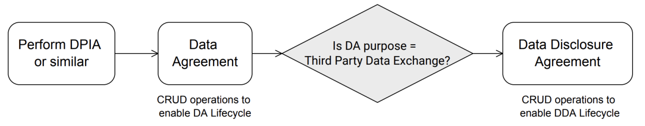

Perform DPIA or similar
Data Agreement
CRUD operations to enable DA Lifecycle
Is DA purpose = Third Party Data Exchange?
Data Disclosure Agreement
CRUD operations to enable DDA Lifecycle

Fig. 2. High-level Data Exchange Agreement Workflow

The data agreement has its own lifecycle, implemented by its CRUD operations.

In cases where the purpose of processing is towards third-party data exchange, a DDA is formulated and published, e.g. towards a dataspace ecosystem, to make endpoints and services discoverable. Once discovered, DS and DUS can dynamically enter into data-sharing agreements to share and reuse personal data across organisational boundaries.

Like DA, the DDA has its own lifecycle, implemented by CRUD operations. Both DA and DDA have a similar lifecycle, as illustrated in Fig. 3 below.

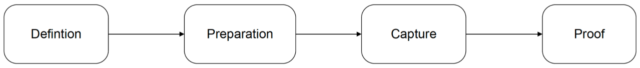


Fig. 3. Phases of DA and DDA lifecycle

The different lifecycle phases are explained below:

Definition: An existing agreement template is adopted as is, or new ones are formulated in this phase. The template could be based on a particular industry and sector-specific practice. This can then be used by any organisation (DS or DUS) for a particular data usage purpose, in our case, for enabling third-party data exchange.

Preparation: An organisation creates an agreement based on a DPIA or similar and shares it with relevant parties. The relevant counterparty for the DA is the individual, and it is a DUS for the DDA.

Capture: The counterparty signs the agreement in this phase. For a DDA, it is countersigned by the DUS, while for a DA, it's the individual. The parties can also reject or revoke an agreement in this phase.

Proof: Any organisation or individual can demonstrate that an agreement exists between the parties. Independent auditors can also check that records are in place, proving that the individual's personal data may be processed (e.g. as per Article 30, GDPR Article 30 [8]).

H. *Key values of Data Exchange Agreements*

The key values enabled by DEXA are as described below:

- *Data regulatory compliance*: A DA based on a DPIA, together with a DDA, provides reassurance that the organisation has the intent to exchange data in compliance with a jurisdiction appropriate data protection regulation.

- *Transparency*: A DA provides the requisite transparency to an individual on how personal data is to be used by an organisation, especially if exchanged with third parties. DDA enables organisations to be transparent about their data usage towards individuals, auditors and other organisations.

- *Auditability*: With a DA and DDA, a DS can prove its legitimate right to collect and share data with a DUS via a digital token-based verification system. Similarly, an individual can dispute data usage for which no legitimacy can be proven using the signed DA. DS and DUS can comply with regulations, e.g. GDPR Article 30 [8].

- *Human-centricity*: The focus is empowering individuals to control their data and make informed decisions about its use. It provides mechanisms to opt-in and opt-out in case consent is used as a lawful basis.

- *Clarity and simplicity*: Using clear and concise language to make data exchange agreements understandable for all parties involved.

- *Flexibility and scalability*: The ability to adapt to changing business needs and emerging technologies while ensuring compliance and security.

IV. IMPLEMENTATION

I. *Implementation set up*

Fig 4 provides the reference implementation used to evaluate the capabilities of data exchange agreements. It uses self-sovereign identity and verifiable credential technologies.

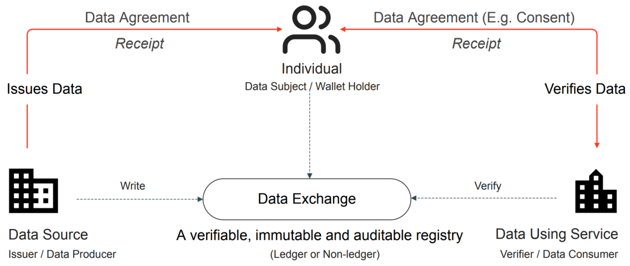


Fig. 4. Reference implementation with data agreements

In this implementation setup, the personal data exchange occurs through a series of interactions between the DS (issuer), the holder, and the DUS (verifier). The exchange process involves the following steps:

1. The individual requests personal data from the DS.

2. The DS verifies the holder's identity and grants the requested personal data access. To keep the records of all processing, the issuer uses a data agreement, signs it and presents it to the individual.

3. The individual receives personal data, views the signed data agreement, and counter-signs it to accept and store it in their digital wallet.

4. The DUS requiring data processing sends a request to an individual with a signed data agreement specifying the terms and conditions for sharing the data.

5. The individual views the request and the signed data agreement and counter-signs it to share the data. The DUS can now use the data for its intended purposes.

This implementation setup follows the principles of data minimisation and consent-based data sharing (if consent is used as the lawful basis), ensuring that personal data is only shared for specific, legitimate purposes and with the explicit agreement of the data holder. The DS/DUS and the individual retain a signed data agreement receipt which can be used towards audits. With the receipt, the DS/DUS can fulfil their obligations under Article 30 of the GDPR (Records of processing activities) [11].

The implementation uses the Decentralised Identifier Communication (DIDComm) messaging protocol [12] between issuers, holders, and verifiers in a personal data exchange setup. It allows for a secure exchange of verifiable credentials or proofs, which the DUS can verify cryptographically. This messaging protocol is privacy-preserving, as it does not require the exchange of personal data but only the exchange of verifiable credentials that attest to the authenticity and integrity of the data. Additionally, DIDComm messaging is decentralised and relies on a peer-to-peer network, adding an extra layer of security to exchanging sensitive personal data. This messaging protocol is beneficial in healthcare settings, where the exchange of sensitive personal data is frequent, and privacy concerns are paramount. Implementing DA and DDA protocol [13] using DIDComm is open-sourced and available for audit for anyone interested.

J. Verifiable Presentations with DIDComm

A verifiable presentation is a subset of one or more verifiable credentials. Instead of sharing all the information in the verifiable credential, an individual (holder) can selectively disclose only the necessary information to a DUS (verifier). Verifiable presentations can be exchanged between a holder and a verifier using the DIDComm messaging protocol. The individual can review the presentation and approve or deny its release to the DUS through a secure Present-Proof DIDComm Protocol [14]. The DUS can then verify the authenticity of the presentation using the issuer's public Decentralised Identifier (DID) and the cryptographic proof embedded in the presentation. This process allows for secure and auditable data exchange while protecting the privacy of the individual's personal information.

K. DEXA protocol implementation

All agreements in the DEXA landscape use JSON-LD serialisation format and conform to W3C Verifiable Credential Data Model [8]. Besides the metadata for data policy, the agreements also contain cryptographic proofs or signatures that ensure its integrity. The following design requirements are met to embed the signatures in the agreement:

1. Can embed multiple signatures so the signing and counter signing can happen during the prepare and capture phases of the data agreement life cycle.

2. Preserve the order of the signatures by protecting the chronology or the chain of events during a signing process. This also ensures non-repudiation so neither of the parties cannot deny the validity of their signatures.

Signature Process: Agreements rely on W3C Data Integrity [15] specifications to embed the signatures and satisfy the above design requirements.

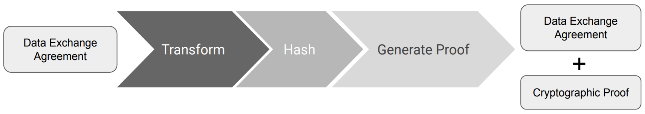


Fig. 5. Workflow for embedding cryptographic proofs in the agreements

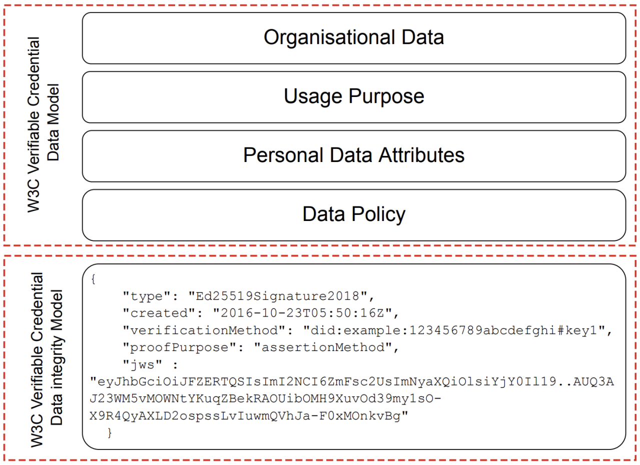
To create a cryptographic proof of the agreements, the following steps are required:

1. Transform data: The agreement is converted to canonicalised n-quads statement using the URDNA2015 canonicalisation algorithm.

2. Hash data: The agreement is hashed using the SHA256 hashing algorithm

3. Generate proof: The proof is generated and serialised per the W3C LDS ED25519-2018 signature suite [16].

Data Exchange Agreement Signature Data Model: The data agreement schema is illustrated in Fig. 6. The agreement data model has two parts: 1) W3C Verifiable Credential Data Model, which encompasses the organisational data (Organisation name, location, industry sector etc.), the usage purposes (purpose, purpose description, lawful basis etc.), personal data attributes (name, age, pulse reading or any PII attribute) and the data policy (e.g. retention period, policy URL, storage location, jurisdiction etc.). The DA and DDA ontology or data vocabulary is published in references [17] and [18] and can be resolved dynamically online.


W3C Verifiable Credential Data Model
Organisational Data
Usage Purpose
Personal Data Attributes
Data Policy
W3C Verifiable Credential Data integrity Model

```
{
    "type": "Ed25519Signature2018",
    "created": "2016-10-23T05:50:16Z",
    "verificationMethod": "did:example:123456789abcdefghi#key1",
    "proofPurpose": "assertionMethod",
    "jws" :
"eyJhbGciOiJFZERTQSIsImI2NCI6ZmFsc2UsImNyaXQiOlsiYjY0Il19..AUQ3A
J23WM5vMOWNtYKuqZBekRAOUibOMH9XuvOd39my1sO-
X9R4QyAXLD2ospssLvIuwmQVhJa-F0xMOnkvBg"
  }
```

Fig. 6. Data agreement schema with cryptographic proofs

L. Embedding DEXA into Verifiable Presentation

Today, the DA is implemented via a W3C-specified Decentralised Identifier (DID) `DID:mydata`. Any DUS wishing to consume any personal data prepares a data agreement offer. This offer is embedded into the Verifiable Presentation request as an extension of the Decorator protocol [19].

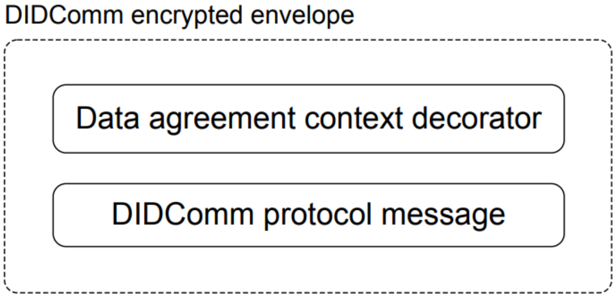


Fig. 7. DIDComm protocol message with data agreement context decorator

Here, agents conform to Aries Interop Profile (AIP) 1.0 [20], cloud or mobile-based, and share a verifiable presentation with a DUS through the Present Proof protocol [21]. The data agreement offer is embedded into the presentation request message using a data agreement context decorator [22], as illustrated in Fig. 7.

When Data Wallet (or any other digital wallet supporting AIP 1.0) receives the presentation request message, it first checks if there is a DA context decorator present. If the decorator is present, the Individual is notified, and they can inspect the DA. If the Individual accepts the DA, it is counter-signed and sent back with shared data to the Data Using Service organisation. However, the Individual also has the option to reject the DA during this process.

Overall, this approach provides a secure and transparent way for individuals to share their data with trusted Data Using Service organisations while ensuring that the terms of any data agreements are clear and verifiable.

V. CASE STUDY AND EVALUATION

M. Health data exchange for remote patient monitoring

In this case study, the DEXA protocol was utilised within a healthcare setting that provides remote patient monitoring for elderly patients. The patients could engage in a video conference call with their caregiver (doctor) and verify their identity online using secure authentication measures. To ensure regulatory compliance and private communication, DEXA established a secure data agreement between the patient and the caregiver.

Before the conference call, the patient and the caregiver verify their identity by providing proof of using a secure identity verification system, for example. The system utilised a ledger-based technology with verifiable credentials to ensure the authenticity of the identity credential. Both the patient and the caregivers could view the verified identity credentials.

During the conference call, the caregiver requested access to the patient's medical records, including medication history, health data, and other relevant information. The patient responded to the caregiver's request by agreeing to a data agreement that specified the data to be shared, the purpose and the duration of the agreement. Once the data agreement was established, the patient's medical records were securely transmitted to the caregiver. The caregiver used the patient's medical records to provide personalised health and care advice and to make informed decisions about the patient's health.

The case study demonstrated the potential of DEXA to enable data exchange in healthcare, enabling remote patient monitoring systems designed for the elderly. Using DEXA, we can protect sensitive patient data while still providing access to relevant data for healthcare professionals to generate actionable insights and provide high-quality care. The patient can view the data exchanged clearly and transparently, and both parties have a copy of the data agreement receipt. The receipt also allows the caregiver organisations to comply with regulations while fulfilling their obligations [13].

N. Passport data exchange

The Data Wallet developed by iGrant.io [23] offers a convenient and secure solution for exchanging passport data. With this tool, individuals can easily convert their NFC-enabled passports into verifiable credentials that can be shared without compromising the integrity and security of their personal information. One significant use case for this functionality is age verification, which can be effectively performed using Zero Knowledge Proof (ZKP) techniques [24]. By using iGrant.io's Data Wallet, individuals can prove their age without revealing their actual date of birth. The verifiable credential contains only the necessary information to verify their age or prove they are above a certain age. The Data Wallet employs a self-sovereign identity approach, which gives individuals complete control over their data and enables them to share it only with trusted parties, thereby providing a secure, privacy-preserving way of sharing personal data.

In the case example, a DUS formulates the data agreement, e.g., checking an individual's age based on one's passport. The DUS signs the DA and presents it along with the data request, which is counter-signed by the individual while accepting to share data. The individual can view the data exchanged, and both parties have a signed copy of their data agreement receipt in their digital wallets.

O. Limitations of Data Exchange Agreements

The proposed DEXA protocol suite shows promising results in our evaluation. It provides a framework for building trust in a scalable data exchange infrastructure, meeting all key values it enables. The use of DPIA as an input to the DEXA lifecycle is also coherent with existing industry practices. It is, however, important to acknowledge its limitations. These include the need for standardisation, wider protocol adoption, and potential challenges in implementation and integration with existing systems. However, the overall positive impact of DEXA on promoting transparency and accountability in personal data transactions cannot be denied.

A major drawback is that DEXA requires trust between parties and relies on their ability to enforce the terms of the agreement. If there is a lack of trust or enforcement mechanisms, the DEXA may not effectively achieve its goals. The performance of digital signatures is a perceived issue. However, research shows that [25], the signature algorithm Ed25519 we used in the reference implementation DEXA framework, is at par with known IT systems. Another alternative is to use ECDSA p-256 signature algorithm compliant to address the concerns related to senior official's group information systems security (SOG-IS) agreed cryptographic mechanisms [26].

VI. RELATED WORK

While some of the related work focuses on specific technologies, such as blockchain [27][28] or distributed ledger, the approach taken in the Data Exchange Agreement (DEXA) described is technology-agnostic. For example, the paper by C. Choi, J. Lee, and H. Kim [27] proposes a blockchain-based secure data-sharing system for Industry 4.0 to ensure the integrity and confidentiality of data exchanged between devices and machines. The system is based on a private blockchain and uses smart contracts to enforce data access and sharing rules. The proposed system is evaluated using a use case of a smart factory, and the results show that it can provide secure and efficient data sharing among different parties in the ecosystem.

The paper by Gao et al. [28] proposes a blockchain-based system for patient information exchange that preserves privacy by allowing patients to control their data. The proposed system uses smart contracts to enforce privacy policies and allows patients to control access to their data through a consent management module. The system was designed to comply with relevant privacy regulations and was evaluated using simulated healthcare scenarios. The results showed that the proposed system effectively preserved patient privacy while enabling secure and efficient data exchange between healthcare providers.

The research gap addressed in the paper is the challenge of effectively implementing data privacy measures and ensuring regulatory compliance in the context of digitalisation. The paper proposes a comprehensive data exchange framework that bridges this gap by incorporating risk-based compliance, human-centric consent acquisition (via data agreements), and cryptographic mechanisms for secure and auditable data sharing. Moreover, DEXA can be applied to the ledger and non-ledger solutions and centralised and decentralised systems. This approach allows for greater flexibility and wider applicability, making the DEXA a valuable tool for data exchange and digital rights management across various industries and use cases. By focusing on the agreement rather than the underlying technology, the DEXA may be more easily adaptable to future data exchange and digital rights management developments. It is also worth noting that DEXA provides a standardised framework for data exchange between organisations, which can include healthcare organisations and be extended to other industries, mobilising the use of data across industry sectors. Most importantly, the DEXA data policy is aligned with the proposed ISO27560 standard [29] on data privacy.

VII. CONCLUSION

In conclusion, in today's data-driven world, data exchange agreements are essential for ensuring auditable data exchange and responsible digital rights management. With the increasing demand for secure and trustworthy data exchange, implementing a data exchange protocol in digital wallet-based data ecosystems can provide a viable, transparency-centric solution [7] to some of the more pronounced digitalisation challenges outlined earlier in the introduction [2][3][4]. The DEXA framework proposed in this paper offers a comprehensive approach to data exchange agreements, enabling stakeholders to exchange data transparently, accountably, and securely.

By adopting the DEXA framework, organisations can minimise non-compliance with regulations such as GDPR, retain control over their data, and establish trust with their partners and customers. As the importance of data access and reuse continues to grow, adopting the DEXA framework can lead to a more transparent and trustworthy data exchange ecosystem, benefiting both organisations and individuals alike.

To summarise, the DEXA framework addresses the key challenges identified in the introduction related to data privacy, regulatory compliance, transparency, and auditability in data exchange. By providing a practical approach that incorporates risk-based compliance and a human-centric and usable approach to obtaining consents or agreements, combined with cryptographic mechanisms to ensure transparency and auditability, the DEXA framework offers a promising solution for responsible and secure data exchange.

REFERENCES

[1] European Parliament and Council of the European Union. (2016., Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC

[2] Hinds, J., Williams, E. J., & Joinson, A. N. (2018). "It wouldn't happen to me": Privacy concerns and perspectives following the Cambridge Analytica scandal. International Journal of Human-Computer Studies, 118, 46-52

[3] iGrant.io (2018), Whitepaper: “Data Sharing and Consent Management: Making consumer choice a business opportunity”, Accessed April 2003, https://igrant.io/papers/iGrant.io_DataSharing_and_Consent_Management_v1.pdf

[4] Lindgren, P. (2018). GDPR Regulation Impact on Different Business Models and Businesses.Journal of Multi Business Model Innovation and Technology, Vol 4(3), 41-56.

[5] Kozlowska, I. (2018). Facebook, Data Privacy, and the Age of Cambridge Analytica. The University of Washington - Jackson School of International Studies

[6] Schwartz, D.G., Weber, S., Weichert, T. et al. (2016) Transparency in Data Processing on the Internet. Joint Proceedings of Ongoing Research of IFIP EGOV and IFIP ePart 2016. IOS Press

[7] Bonatti, P., Kirrane, S., Polleres, A., & Wenning, R. (2017). Transparent Personal Data Processing: The Road Ahead. In 3rd International Workshop on Technical and Legal Aspects of Data Privacy and Security

[8] Verifiable Credentials Data Model v1.1. Sporny, M; Noble, G; Longley, D; Burnett, D; Zundel, B; Den Hartog, K. (2022), W3C Recommendation, Available at: https://www.w3.org/TR/vc-data-model

[9] European Commission (2021). "European Digital Identity", Accessed April 23, 2023, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en

[10] Lessig, L. (2006) "Code and Other Laws of Cyberspace, Version 2.0", New York: Basic Books

[11] GDPR. n.d. "Article 30: Records of processing activities." Accessed April 25, 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e1682-1-1

[12] Decentralised Identity Foundation (2022). "DIDComm Messaging v2.0." Accessed April 30, 2023. https://identity.foundation/didcomm-messaging/spec/v2.0

[13] Data Exchange Agreements (2021). Decentralised Data Exchange GitHub Repository. Accessed 01-May-20023. https://github.com/decentralised-dataexchange/data-exchange-agreements

[14] Khateev, N. (2019). Aries RFC 0037: Present Proof Protocol 1.0, Accessed May 02, 2023, https://github.com/hyperledger/aries-rfcs/tree/main/features/0037-present-proof

[15] Sporny, Manu and Longley, Dave. Credentials Community Group. n.d. "Data Integrity." CG-DRAFT. Accessed April 30, 2023. https://w3c-ccg.github.io/data-integrity-spec/

[16] W3C Credentials Community Group (2018). "Ed25519 Signature 2018." Accessed April 30, 2023. https://w3c-ccg.github.io/lds-ed25519-2018

[17] iGrant.io. n.d. "Data Agreement Vocabulary." Accessed April 2023. https://docs.igrant.io/docs/data-agreements-versions

[18] iGrant.io. n.d. "Data Disclosure Vocabulary." Accessed April 2023. https://docs.igrant.io/docs/data-disclosure-agreements-versions

[19] Hardman, D (2020). Aries RFC 0011: Decorators, Accessed April 30, 2023. https://github.com/hyperledger/aries-rfcs/tree/main/concepts/0011-decorators

[20] Hyperledger Aries. (2022). Aries Interop Profile. Accessed April 2023 https://github.com/hyperledger/aries-rfcs/blob/main/concepts/0302-aries-interop-profile

[21] Hyperledger Aries RFC 0037 (2019), "Present Proof Protocol 1.0", Accessed April 30, 2023. https://github.com/hyperledger/aries-rfcs/tree/main/features/0037-present-proof

[22] Automated Data Exchange RFC-006 (2022), “Data Agreement Context Decorator”, Decentralised Data Exchange GitHub repository: https://github.com/decentralised-dataexchange/automated-data-agreements/tree/main/ada-rfcs/rfc-006

[23] iGrant.io. n.d. "Data Wallets." Accessed April 30, 2023. Available for download at Playstore and Appstore via https://igrant.io/datawallet.html

[24] Goldreich, O., Micali, S., & Wigderson, A. (1986). Proofs that yield nothing but their validity and a methodology of cryptographic protocol design. In Proceedings of the 27th Annual Symposium on Foundations of Computer Science (SFCS 1986) (pp. 174-187). IEEE.

[25] Faz-Hernández, A., Fujii, H., Aranha, D. F., & López, J. (2017). A Secure and Efficient Implementation of the Quotient Digital Signature Algorithm (qDSA). Institute of Computing, University of Campinas. 1251 Albert Einstein, Cidade Universitária, Campinas, São Paulo, Brazil.

[26] SOG-IS. (2020). Agreed Cryptographic Mechanisms (Version 1.2), Available at: https://www.sogis.eu/documents/cc/crypto/SOGIS-Agreed-Cryptographic-Mechanisms-1.2.pdf

[27] C. Choi, J. Lee, and H. Kim, "Blockchain-Based Secure Data Sharing System for Industry 4.0," in Proceedings of the 2018 International Conference on Information and Communication Technology Convergence (ICTC), Jeju Island, Korea (South), Oct. 2018, pp. 899-901

[28] Gao J, Zhou H, Tang J, et al. (2022). Privacy Preservation in Patient Information Exchange Systems Based on Blockchain: System Design Study. Journal of Medical Internet Research 2022;24(3):e29108

[29] International Organization for Standardization. (2019). Privacy technologies — Consent record information structure: Draft Technical Specification, ISO/IEC DTS 27560. Geneva, Switzerland.