# The Right to be Forgotten Meets the Immutable

## A Practical Guide to GDPR-Compliant Blockchain Solutions

THE CENTER FOR
GLOBAL ENTERPRISE

CRAVATH, SWAINE & MOORE LLP

DSCI
DIGITAL·SUPPLY·CHAIN·INSTITUTE

SLAUGHTER AND MAY

# Contents


p3
**Preface**

p4
**A Practical Guide to GDPR-Compliant Blockchain Solutions**

p6
**Guiding Principles**

p7
**1 An Introduction to Blockchain**

p8
**2 An Introduction to the Relevant GDPR Requirements**

p10
**3 How Blockchain Can Meet the GDPR Challenge**

3.1 Keep personal data off the Blockchain p10

3.2 Establish a robust contractual governance framework p12

3.3 The Grand Challenge: The deletion of data and exercising of data subject rights p13

p16
**4 The Shipping Industry, Blockchain, and GDPR: The MTI Case Study**

p17
**5 Conclusions and Key Takeaways**

# Preface

Blockchain and Distributed Ledger Technologies (DLT) have emerged as an effective enterprise transformation tool. They provide capabilities beyond traditional databases to share data and manage workflow throughout an enterprise and across its ecosystem of customers, partners and suppliers in a trusted manner without central control.

As with many exciting new technologies, the hype surrounding Blockchain has been extreme and prompted a tidal wave of company experimentation that has proven one thing: Blockchain is not a good fit for all applications, but for some, it is an exceptional fit. It is our belief that many supply chain operations belong in the exceptional category. The Center for Global Enterprise's (CGE) Digital Supply Chain Institute's (DSCI) research has shown that with proper selection of use-cases, tremendous benefits can be realized[1].

Blockchain for the enterprise is a specialized workflow automation tool that when applied properly is a powerful cross-enterprise transformation instrument. However, our research has shown that success stories remain elusive because of difficulties in forming the Blockchain ecosystem or network, determining network and data governance, and complying with government data regulations. It is this last element that forms the basis of this paper.

Many commentators have written that GDPR and Blockchain technology are fundamentally incompatible. This paper was prompted by DSCI members who saw this as a clear inhibitor to Blockchain adoption and asked for our view. We enlisted the intellectual property, technology and data protection practices of Cravath, Swaine & Moore and Slaughter and May, two leading international law firms, to better define the opportunities and challenges as the new law applies to this nascent technology. This paper is an abridged version of the full paper "*March of the blocks: GDPR and the blockchain*" written by the same parties[2].

Other countries will, undoubtedly, adopt regulations similar to GDPR and hence businesses are unlikely to avoid privacy compliance issues in the future. We also want to emphasize that the GDPR is a pressing concern not just for B2C companies, as the evolution of supply chains in a digital economy is increasingly making B2C and B2B distinctions irrelevant. We also note that a simple signature on a purchase order can be subject to the regulation, making it relevant to all businesses.

In this paper, we focus on GDPR compliance in a Blockchain network. We will examine the power and efficiencies Blockchain brings to the shipping industry and examine the compliance challenges created by GDPR. We conclude that GDPR and Blockchain can happily coexist and provide a framework for addressing GDPR compliance in a Blockchain network.

# A Practical Guide to GDPR-Compliant Blockchain Solutions

Over the past decade, Blockchain-based technologies have evolved in a wide range of directions. Businesses have applied increasingly innovative uses of Blockchain technology to a growing range of solutions for recording, processing and sharing information: offering decentralization, accessibility, and reliability. As excitement over some of the most revolutionary aspects of Blockchain technology, such as the distribution of ledger data and its generally immutable nature has grown, governments, regulators, and organizations have increasingly supported Blockchain's potential[2].

> "Very few companies have actually scaled a Blockchain solution. Most companies have done a "Proof of Concept" (POC) but not found a reason to invest in a full Blockchain solution. DSCI's research shows that in almost all of these cases, that the company did not fully understand the potential of Blockchain to increase business value and selected applications where the incremental value was modest. Our concern is that companies will make even less investment in Blockchain because of GDPR concerns. DSCI's view is selecting the right place to increase business value will lead to a scaled-up solution.
> — George Bailey, Managing Director, DSCI

On nearly the same timeline, increased privacy concerns and calls for individuals to have the right to control their personal data coalesced into the EU's recently enacted General Data Protection Regulation (GDPR). Similarly, GDPR has ignited excitement over its most revolutionary aspects, such as the right to have one's personal data deleted or corrected in certain situations.

The GDPR's right to erasure (the so-called "right to be forgotten") naturally poses significant compliance hurdles to the ongoing development of immutable Blockchain-based solutions involving storing and transacting with data about individuals. However, there are additional difficulties associated with achieving a GDPR-compliant Blockchain solution. Indeed, a number of commentators have discussed the tensions between the GDPR and Blockchain technology. Some have even declared Blockchain fundamentally incompatible with the GDPR. While we take a more optimistic view, their concerns are not entirely misplaced.

In our view, these concerns do not render GDPR compliance impossible. In particular, we believe a GDPR-compliant Blockchain solution can exist where that solution involves a defined group of participants, all of whom agree to a common contractual governance framework. However, this will require steps to be taken by regulatory authorities and technology providers, such that the outstanding privacy challenges posed by Blockchain (but not fully addressed by legislation or regulatory guidance) can be solved.

When applied properly, Blockchain is an important cross-enterprise transformation tool. The Center for Global Enterprise (CGE), as part of our mission worked with the law firms Cravath, Swaine & Moore and Slaughter and May to help bring clarity and practical management best practices to this subject. Our work offers suggestions on how best to implement GDPR-compliant Blockchain solutions. We have analyzed some of the key requirements of the GDPR that present a compliance challenge for Blockchain solutions, and have considered how a Blockchain solution can be deployed to meet that challenge.

Rather than offer a theoretical discussion, this paper aims to be of practical use to those seeking to deploy Blockchain solutions in their business by examining a real world use case developed by Marine Transport International (MTI), a UK-based digital logistics company.

While it may not yet be possible to solve all of the challenges posed by the GDPR and other privacy regimes to the implementation of Blockchain solutions, **we do not feel that Blockchain technology and data protection and privacy are inherently contradictory.** Quite the opposite. A Blockchain solution that respects the fundamental principles of data protection and privacy is achievable if the following four guiding principles are followed.

# Guiding Principles

## Use a private, permissioned Blockchain.

While the most common vision of Blockchain is of a fully public, permissionless network, there are many private networks that are in fact private and require permission to join. Because anyone can join a public permissionless Blockchain, it is impossible to ensure participants agree to necessary rules around the protection of personal data. As a result, **the private, permissioned Blockchains can be employed to work towards a GDPR-compliant Blockchain solution.**
(See appendix for Blockchain decision tree.)

## Avoid, if possible, the storing of personal data on the Blockchain.

The most obvious way to avoid GDPR compliance issues is to use a Blockchain solution that does not process any personal data and minimizes free form data storage. While keeping a Blockchain completely free of personal data will be very difficult to achieve, this may be done, for example, by storing an encrypted representation of the personal data on the Blockchain, with the underlying and identifiable personal data being kept off-chain. Middleware can then be used to combine off-chain and on-chain data to provide a complete view to authorized users that includes the off-chain personal data to authorized users.

## Establish a detailed governance framework.

Given: (a) the need to adequately protect personal data; (b) the requirement to establish contractual relationships governing the processing of personal data between parties; and (c) the legal obligations on data controllers to provide individuals with the means to uphold their personal data rights, a GDPR-compliant commercial Blockchain solution will require a governance framework that is contractually binding on all participants and clearly sets out each party's rights and responsibilities.

## Employ innovative solutions to data protection problems.

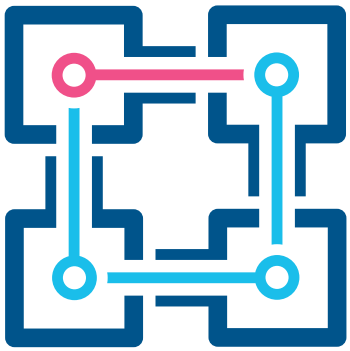
The immutable nature of Blockchain data is the one element of the technology which clashes most obviously with data subjects' rights under the GDPR. However, through use of innovative solutions such as advanced irreversible encryption as a means of deletion, it is possible to comply with the spirit and (we argue) the policy of the legislation, if not yet fully the word. While we believe that there are good arguments for irreversible encryption being adequate for GDPR compliance, definitive guidance from regulatory authorities is necessary in this area to remove doubts caused by the disconnect between legislation, guidance and technological advancement.

Ultimately, we are calling on regulatory authorities to provide guidance on the adequacy of the proposed solutions to the Blockchain GDPR challenges discussed in this paper so that technology providers can move forward with certainty. Indeed, regulators recognize[5] that if guidance is not provided, there is a risk of a stall in or even end to investments into Blockchain companies who are developing solutions that could, in the long run, benefit global commerce.

Finally, it should be noted that this publication is intended for general information only and is not intended to provide legal advice.

# 1 An Introduction to Blockchain

A Blockchain is a series of blocks of data that are linked together in a secure fashion by what is known as a "cryptographic hash." Each block of data in the chain scrambles bits of information from the previous block into a "hash." Because the previous block in the chain includes a hash of the block before that one (and so on back to the first block), the blocks form a continuous, secure or -- immutable chain. This is one of the cornerstones of Blockchain technology and is at the heart of what guarantees the reliability and integrity of Blockchain networks.



In addition, there is the concept of a distributed ledger. A distributed ledger is a database that is stored separately and maintained independently yet synchronously by consensus, across multiple points (nodes) on a network. Most, but not all, distributed ledgers are implemented using a type of Blockchain.

Where a distributed ledger employs Blockchain technology, each copy of the Blockchain serves as a copy of the ledger and multiple nodes on the network will each have a copy. Thus, when one copy of the Blockchain is modified, everyone else with a copy of the Blockchain (i.e. every other node on the distributed ledger network) can detect that modification because the hash of the latest block of the modified chain will be different than that of the latest block of their own chain.

The greater the number of nodes, the more difficult it is to modify the Blockchain maintained by a majority of nodes, and therefore modify the ledger. Once included in a Blockchain, data is generally immutable: it cannot be changed, and it cannot be deleted (at least not in the traditional sense of the word). It is this aspect of Blockchain technology that most obviously runs against the aims of the GDPR, which has individuals' rights to correct and delete their own personal data at its very core.

While the concepts of a **"Blockchain"** and a **"distributed ledger"** are distinct, in this paper we use the term **"Blockchain"** to refer to a distributed ledger which is implemented using Blockchain technology.

# 2 An Introduction to the Relevant GDPR Requirements

The GDPR is a European Union regulation on data protection and privacy that was implemented in May 2018 and marked a significant evolution in data protection law in Europe.

While the GDPR governs how personal data relating to individuals inside the European Economic Area (the EEA) may be processed, it also has a wide-ranging extra-territorial application. The GDPR applies first and foremost to entities that are processing personal data in the context of a European establishment, regardless of whether or not the processing takes place in the EEA. Additionally, the GDPR can also apply to entities established outside the EEA that are offering goods or services to (or monitoring the behavior of) individuals in the EEA.

Given that the GDPR is generally perceived as a high-watermark of international data protection laws (and becoming a template for other countries' data protection laws), building a GDPR-compliant Blockchain solution will advance worldwide data protection and privacy compliance.

This paper highlights those aspects of the GDPR regulation we consider to be most relevant to the question of compliance for Blockchain solutions.

## Personal data

In relation to the GDPR, personal data is any information relating to an identified or identifiable natural person. It includes names, addresses, identification numbers, location data, and IP addresses. The GDPR also sets out special categories of personal data subject to stricter regulation. This category includes personal data revealing racial or ethnic origins, political opinions, religious beliefs, and health data.

## Processing personal data

The GDPR defines the "processing" of personal data broadly. This effectively captures almost anything one might do with data, including merely storing it. Blockchain solutions that store or share personal data will inevitably be involved in the "processing" of that personal data.

## Controllers and processors

Entities processing personal data under the GDPR fall into two categories: data controllers and data processors. A data controller is an entity that, alone or with another data controller, has primary responsibility for the processing of personal data, and that determines the manner in which, and the purposes for which, the personal data is processed. A data processor, on the other hand, processes personal data on behalf of a data controller, under mandatory contractual provisions set out in the GDPR. In a Blockchain ecosystem, where decentralization is key, the variety of stakeholders makes the controller/processor differentiation complex.

## Privacy by design

The GDPR's aim through privacy by design is to change organizational attitudes to the protection of personal data by making it a pervasive issue that is considered by organizations as a matter of course during their business as usual practices.

## Rights of individuals

The GDPR provides a set of detailed rights for individuals. Within the context of Blockchain applications, the most pertinent of these are: a) the right to erasure (i.e. the "right to be forgotten"), which gives individuals a right to request that certain (usually outdated) information about them be deleted; and b) the right to rectification, which allows individuals to have incorrect data referring to them corrected.

## International transfers of personal data

Given the global nature of many Blockchain solutions, it is also important to consider the GDPR restrictions on the transfer of personal data outside the EEA. Under the GDPR, personal data cannot be transferred outside the EEA unless: (i) the European Commission has determined that the country to which data is transferred provides an adequate level of protection for personal data (or if the recipient is approved under a scheme such as the EU-US Privacy Shield); or (ii) standard form contractual limitations oblige the transferring parties to provide an adequate level of protection for personal data.

# 3 How Blockchain Can Meet the GDPR Challenge

## 3.1 Keep personal data off the Blockchain

The most obvious way to avoid the application of the GDPR to a Blockchain solution is to avoid processing any personal data as part of that solution. Indeed, one crucial aspect of distributed ledger technology, that data should be replicated and maintained by various participants rather than stored centrally, is at odds with the GDPR's principles of data minimization, storage limitation, and purpose limitation. The ideal means to resolve this dilemma is to avoid it altogether. The breadth of the definition of personal data in the GDPR, however, makes the keeping of all personal data off the Blockchain difficult.

### CHALLENGE: Unique identifiers as personal data.

Personal data can include unique identifiers assigned to an individual such as an IP address or, on a Blockchain network, the address assigned to a participant on the network. In that case, the participant's address on the Blockchain network will be considered personal data under the GDPR.

### SOLUTION: Avoid the use of persistent identifiers for individuals.

If a Blockchain solution is being deployed in a business context, one way to avoid addresses being treated as personal data is to ensure that (if practicable) all participants on the network are bodies corporate rather than individuals.

Another route is to avoid using persistent public addresses for participants. Some Blockchain technologies use cryptography to generate a different address to refer to a participant for each transaction. This helps to obfuscate the identity of participants, making it difficult to piece together different transactions which, when combined with other information, could uncover the identity of the individual.

## CHALLENGE: Inadvertent addition of personal data to the network.

Another way personal data can land on the Blockchain ledger is where substantive data uploaded to the Blockchain as part of a transaction on the network (the transaction payload data) contains personal data. A transaction payload containing an individual's name, address, phone number, email address, or other contact or identifying details will result in that personal data being added to the Blockchain.

## SOLUTIONS:

### Governance.

The first line of defense is to implement a contractual governance framework that obliges individuals not to upload personal data to the network and minimizes free form data uploads. But given the possibility of personal data inadvertently making its way onto the network, this is not necessarily a perfect solution.

### Technical measures to redact personal data (design considerations).

Blockchain middleware applications can prevent the inclusion of specific personal data fields such as names, phone numbers or email addresses. These applications can also employ Artificial Intelligence or Machine Learning-based tools to recognize and remove personal data from information submitted to the Blockchain network, for example, recognizing and blurring faces in images before they are submitted to the network. Some of the most exciting innovation in Blockchain technology is occurring in Blockchain middleware.

### Hashing personal data.

A third way to keep personal data off the Blockchain is to ensure that any data containing personal data is communicated via a side channel, with only a hash of that personal data stored on the Blockchain. However, communicating data via a side channel requires the use of Blockchain middleware to appropriately route data and some debate remains about whether a hash of personal data is anonymous data.

## 3.2 Establish a robust contractual governance framework

### Key GDPR requirements

There are several key requirements of the GDPR which mean that any deployment of a commercial Blockchain network will require a governance framework that is contractually binding on all participants. We consider those requirements to be: (i) detailed data processing agreements as between controllers and processors; (ii) clear and transparent agreements as between joint data controllers (where relevant); (iii) restrictions on transfers of personal data out of the EEA; and (iv) the provision of fair processing information (i.e. privacy notices).

However, as a pre-requisite to any governance framework, it will be necessary to implement GDPR-compliant Blockchain solutions on a private, permissioned network (as opposed to a public, permissionless network). To interact with a private permissioned Blockchain network, participants must first obtain authorization. Private permissioned Blockchain networks employ various processes to approve new participants, including ensuring all new participants subscribe to a set of rules or terms and conditions that govern their use of the network. Because anyone can join a public permissionless Blockchain network, it is not possible to ensure participants agree to contractual terms and conditions before joining, nor is it possible to know the geographic location of members, assess their safekeeping of data or compliance with GDPR and other applicable regulations. For these reasons, compliance with the various GDPR provisions requiring specific contractual obligations mandates the use of a private permissioned Blockchain.

### Key GDPR obligations satisfied via the contractual governance framework

#### Data processing agreements.

There is much debate about whether members who merely operate nodes processing data on behalf of other participants in the network should be considered data processors or data controllers[6]. We note: a) the decentralized nature of Blockchain makes distinguishing between the roles difficult; and b) it is important to determine whether a member is a data controller or a data processor, as the GDPR imposes different responsibilities on each participant classification. A governance framework should clearly identify which members will upload data onto the network (data controllers), and which members only passively participate in the network (potentially mere data processors).

#### Restrictions on transferring personal data out of the European Economic Area.

The GDPR restricts transfers of personal data out of the EEA. However, any global Blockchain solution will likely involve the processing of data outside of the EEA. To resolve this conflict, a governance framework can incorporate the European Commission's model international data transfer clauses, thereby enabling all network members to transfer personal data to other network members regardless of where the members are located.

#### Fair processing notices.

Lastly, the creation of a governance framework can obligate network members to comply with the GDPR, which oblige data controllers to provide data subjects with fair processing information (i.e. privacy notices). The obligation to provide fair processing information is triggered either when personal data is collected directly from the data subject, or when personal data is obtained from someone other than the data subject[7].

## Governance framework: some key data protection and privacy points

From a data protection and privacy perspective, the governance framework should be contractually binding on all participants in the Blockchain network; implement the GDPR-required provisions; establish a process for data subjects to exercise their rights under the GDPR; and provide mechanisms to achieve data minimisation, privacy by design, risk mitigation and permit the removal of personal data that is no longer required (see below).

## 3.3 The Grand Challenge: The deletion of data and exercising of data subject rights

Identifying personal data prior to placing it on the blockchain is challenging. Such mundane items as a signature on a bill of lading, a comment about a lorry driver entering port, or an individual in the background of a shipping container picture are all personal information that under GDPR that must be recognizable, rectifiable if incorrect and deletable when requested. While B2C businesses may have more exposure to holding personal information, as the above examples show, no industry can escape GDPR's broad requirements.

## CHALLENGE: The right of erasure and the obligation to delete data.

As discussed above, the immutability of data on a Blockchain is at odds with a right to erasure or an obligation to delete data. It will be difficult in most cases to be certain that no personal data is stored on the Blockchain. Thus, Blockchain solutions must confront the need to manage personal information in compliance with the GDPR.

## SOLUTIONS:

### Blockchain "pruning."

If the personal data on a Blockchain network must be retained for a certain number of years to satisfy a legal or regulatory obligation, one option may be to "prune" the Blockchain. Pruning is the process of deleting historical blocks on the Blockchain that pre-date a certain point in time. For example, if regulation requires data to be stored for seven years, the Blockchain governance framework could require that all participants in the Blockchain network delete blocks of data that are greater than seven years old.

### Deletion by way of encryption.

Alternatively, it may be possible to delete personal data stored on the Blockchain by irreversibly encrypting the data. Under this approach, the hash values containing the personal data would remain permanently on the Blockchain, but the personal data contained in the hash would be "deleted" from the Blockchain by removing all keys that enable decryption of the hash. An added benefit of deletion by encryption is that it preserves the immutable nature of the Blockchain, as the data on the Blockchain itself is not altered.

### Editable Blockchains.

Editable Blockchains are a new solution that enables the deletion and rectification of data on the Blockchain. They are considered divisive in certain areas of the Blockchain community because they are not immutable, which is seen by some to undermine one of the fundamental premises of Blockchain technology. That being said, we believe it is important at this stage to strike a pragmatic balance between the ideological purity of a Blockchain solution and the commercial need for privacy compliance.

### Deletion by "forking" the Blockchain.

As a last resort, it is possible to "fork" a Blockchain to remove personal data. To fork a Blockchain, a majority of nodes must agree to a new set of initial rules, and then update the software used to run the Blockchain so that a majority of nodes on a Blockchain network agree to the new ledger. As a practical matter, however, forking is a very costly and operationally disruptive technique.

## CHALLENGE: The right of rectification.

A second major challenge posed by the GDPR relates to the right of rectification. This can be thought of as two distinct rights: (a) the right to correct inaccurate personal data; and (b) the right to complete incomplete personal data. If a data subject with inaccurate or incomplete personal data on a Blockchain asks the data controllers to rectify the information, the data controllers must do so. Similar to the right to erasure, the immutable nature of Blockchain technology is seemingly at odds with the right to rectification, especially the right to rectify inaccurate personal data.

## SOLUTIONS:

### Rectification by a supplementary notice.

The GDPR is clear that it is possible to rectify incomplete personal data by supplementing that data with a clarificatory statement. Still, there are obvious difficulties for Blockchain solutions in rectifying incomplete personal data in historical blocks on the chain. This stems from the fact that alteration to historical blocks will impact the entirety of the Blockchain as it then exists. While the rectification may be feasible by way of a clarificatory statement, it is not clear whether the same is true for the rectification of inaccurate personal data under the GDPR.

### The complexity of rectification *illustrated*

Suppose the statement: "*Ms. X has entered internationally sanctioned Country Y on a business visa*" is recorded in your database. If this statement about Ms. X is incorrect and Ms. X and her business are, in fact, prohibited under international sanctions from conducting business in Country Y, Ms. X might reasonably submit a request to you that the incorrect statement be corrected. It is by no means certain that a regulator or a court would regard it as a sufficient rectification if you were simply to update your database to say: "*Ms. X did not enter Country Y on a business visa. This statement is actually incorrect; Ms. X has not done business in a country subject to international sanctions.*" Indeed, Ms. X may not be satisfied with this and demand that all evidence of the initial statement to be deleted and replaced with a correct statement.

By contrast, however, there may be cases where it is not appropriate to erase personal data, even if incorrect, in order to replace it with correct information. One example is data that serves an evidential purpose, such as a signed contract. It may not be appropriate to modify a signed contract to, for example, correct a mistake in the job title of an individual named in the contract. It may be preferable to attach a clarificatory statement to the contract, so that the contract can still serve as evidence of the exact, unaltered terms of the agreement the parties to the contract reached.

Unfortunately, this is an area where there is no reliable guidance from regulators, and this makes it a further issue that we would urge the relevant regulatory bodies to provide clear guidance on.

## Rectification by deletion.

To the extent it is not possible to comply with the obligation to rectify incorrect personal data by a supplementary statement, it would be necessary to look to the methods outlined above to enable deletion of incorrect the personal data (for example, deletion by encryption) followed by addition of the correct personal data to the Blockchain. Because a data subject might request that incorrect personal data about them of any age be rectified, pruning of the Blockchain may not offer an effective solution.

Pending guidance from data protection regulators that in certain circumstances a supplementary statement may suffice, it is prudent to ensure any GDPR-governed Blockchain solution facilitates the effective deletion of incorrect personal data and permits correct personal data to be added in its place.

# 4 The Shipping Industry, Blockchain, and GDPR: The MTI Case Study

The global shipping industry is struggling to keep pace with the rapid and demanding growth requirements placed on it by the increasing demand for goods of international origin. The systems currently in use are prone to disjointed flows of information, lack of standardization among international logistics databases and the inability/unwillingness to appoint a centralized aggregator to ensure seamless transfer and usage of data and records. All these factors are estimated to cost the industry 10% of global shipping costs each year.

This scenario is the perfect opportunity for the implementation of Blockchain based solutions to enable participants to communicate with each other based on a single shared view of applicable data. Information can be shared in a trusted and consistent way that is auditable and provides "one-source of truth," without the need for any centralized aggregator. However, due to the new GDPR rules, there are several challenges that arise from the restrictions placed on data gathering and handling.

## MTI's GDPR-compliant Blockchain solution:

> "As a result of this research, we now know that Blockchain and GDPR can coexist and have clear understanding on how MTI can design for data privacy, thereby ensuring GDPR compliance."
> — Jody Cleworth, CEO, MTI

MTI has designed a solution which involves an additional piece of software – a middleware application that controls the transfer of data from the users to the Blockchain. It causes sensitive data to be rerouted via and stored separate from the Blockchain and helps with associating this side-channel data with the Blockchain records. MTI plans to establish, together with a consortium of industry players, one such Blockchain network for use in international shipping in line with the GDPR principle of data minimization. Here are the key features of MTI's solution:

- Middleware software interfaces to multiple Blockchain networks, each following their own architectures and regulatory compliances. This allows for each party to run multiple networks as per their need in parallel.
- Artificial Intelligence and Machine Learning integrated into middleware to enhance GDPR compliance and network governance.
- Use of private permissioned Blockchains to ensure adequate access control.
- Restricts personalized and prohibited data from being uploaded onto the Blockchain to limit the opportunities for personal data to enter the network.
- Privacy by design ensures that the system acquires only the adequate and necessary amount of data in any situation and curbs unnecessary information fields. Thus, ensuring a reduction in data liability.
- Creates a transparent and open governance framework that is adhered to by all users.
- Inhibits accessing data in a non-compliant manner.

# 5 Conclusion and Key Takeaways

Through this publication, we have identified that, while it may not yet be possible to solve all of the challenges posed by the GDPR to the implementation of Blockchain solutions, progress can be made if the interested parties work together openly and pragmatically.

**We believe that a Blockchain solution that respects the fundamental principles of data protection and privacy is achievable**, and the four key elements necessary to achieve that aim, as identified in this publication are:

1. Use of a private, permissioned Blockchain.
2. Avoid, if possible, the storing of personal data on the Blockchain. Eliminate/minimize free form data fields.
3. Implement a detailed governance framework.
4. Employ innovative solutions to traditional data protection problems.

We conclude by repeating our call on regulatory authorities to take the steps necessary to address the outstanding privacy challenges posed by Blockchain technology, most importantly, in relation to the use of encryption as a means of anonymisation and deletion of personal data. Innovative solutions to data protection challenges will only succeed with the understanding and support of regulators and lawmakers.

There is a risk that, if steps are not taken by regulators and lawmakers to bridge the gap between data protection law and Blockchain technology, we will witness a slowing in (or even end to) advancements in the area of Blockchain solutions. Such an outcome would ultimately be detrimental to technological developments that may have the capacity to deliver substantial benefits to the world as a whole.

The Center for Global Enterprise (CGE) is a nonprofit, nonpartisan research institution devoted to the study of global management best practices, the contemporary corporation, and economic integration.

CGE's Digital Supply Chain Institute (DSCI), a leading-edge research institute, is focused on the evolution of enterprise supply chains in the digital economy. Blockchain is a major focus area.

Cravath, Swaine & Moore LLP and Slaughter and May are widely recognized as two of the world's leading law firms. They bring legal expertise and business judgment to a range of matters involving the rapidly evolving landscapes of emerging technology, artificial intelligence, data protection and privacy, blockchain and e-commerce.

## Acknowledgements

**Authors: Shawn Muma, David Kappos, Rob Sumroy**

This paper was written by the Center for Global Enterprise (CGE) and leading international law firms Slaughter and May and Cravath, Swaine & Moore LLP. It is published with thanks to Jody Cleworth and his team at Marine Transport International (MTI), for allowing us to use MTI as a case study.

Shawn Muma is the Blockchain research leader at the CGE's Digital Supply Chain Institute. Enterprise Blockchains are a prime focus of his research.

David Kappos is a partner at Cravath, Swaine & Moore and is one of the foremost lawyers in the field of intellectual property. He also led the U.S. Patent and Trademark office (USPTO) from 2009-2013.

Rob Sumroy is a partner at Slaughter and May and is co-head of the firm's global data protection and privacy practice, as well as leading Slaughter and May's technology, emerging technology and cyber advisory units.

We thank CGE team members Sugathri Kolluru and Ira Sager for their suggestions and contributions. We also thank Jessica Goodman, Ryan Wichtowski from Cravath, Swaine & Moore and Ian Ranson, Duncan Mykura from Slaughter and May for their significant contribution, expertise and insights that greatly enabled this research.

## References

[1]Shawn Muma, Are You Fit for Blockchain? Supply Chain Management Review, 18 Dec 2018, available at: https://www.scmr.com/article/are_you_fit_for_blockchain

[2] "European Commission launches the EU Blockchain Observatory and Forum" European Commission press release (1 February 2018), available at: http://europa.eu/rapid/press-release_IP-18-521_en.htm.

[3] French National Commission on Informatics and Liberty (CNIL), "Blockchain and the GDPR: responsible solutions regarding the presence of personal data", 24 September 2018, available at: https://www.cnil.fr/en/node/24807.
German Blockchain Federation (Blockchain Bundesverband), "Blockchain, data protection and the GDPR", 25 May 2018, available at: https://www.bundesblock.de/wp-content/uploads/2018/05/GDPR_Position_Paper_v1.0.pdf.
EU Blockchain Observatory and Forum, "Blockchain and the GDPR", 16 October 2018, available at: https://www.euBlockchainforum.eu/reports.

[4] Gabrielle Orum Hernández, Why Blockchain Poses an Unusual Challenge for GDPR Compliance, LAW.COM, 25 May 2018, available at: https://www.law.com/2018/05/25/why-Blockchain-poses-an-unusual-challenge-for-gdpr-compliance/?slreturn=20181103145145;
Tom Cox and Andrew Solomon, Block chain: Is the GDPR out of date already?, Lexology, 30 August 2017, available at: https://www.lexology.com/library/detail.aspx?g=d4c0481a-c678-4748-80cb-4ab917e66207.

[5] European Parliament Opinion of the Committee on Civil Liberties, Justice and Home Affairs on Blockchain: a forward- looking trade policy available at: http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A8-2018-0407&language=EN - top

[6] EU Blockchain Observatory and Forum, "Blockchain and the GDPR", 16 October 2018, available at: https://www.euBlockchainforum.eu/reports.

[7] Emma McClarkin on Blockchain: a forward-looking trade policy, 27 November 2018, available at: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A8-2018-0407+0+DOC+PDF+V0//EN

# Appendix

## Blockchain Implementation Decision Tree

Blockchain is a specialized workflow automation tool that is particularly effective when applied to cross-enterprise transformation. Below is a use decision making rubric that assists executives and business leaders in determining how to apply blockchain in an environment of GDPR.

**Do:**

- Determine what type of data you are processing
- Determine what regulations this processing triggers
- Follow industry best practices for data processing

**Don't:**

- Use a public blockchain to implement a solution that uses personal data
- Permanently store personal data on-chain
- Ignore regulatory guidance documents