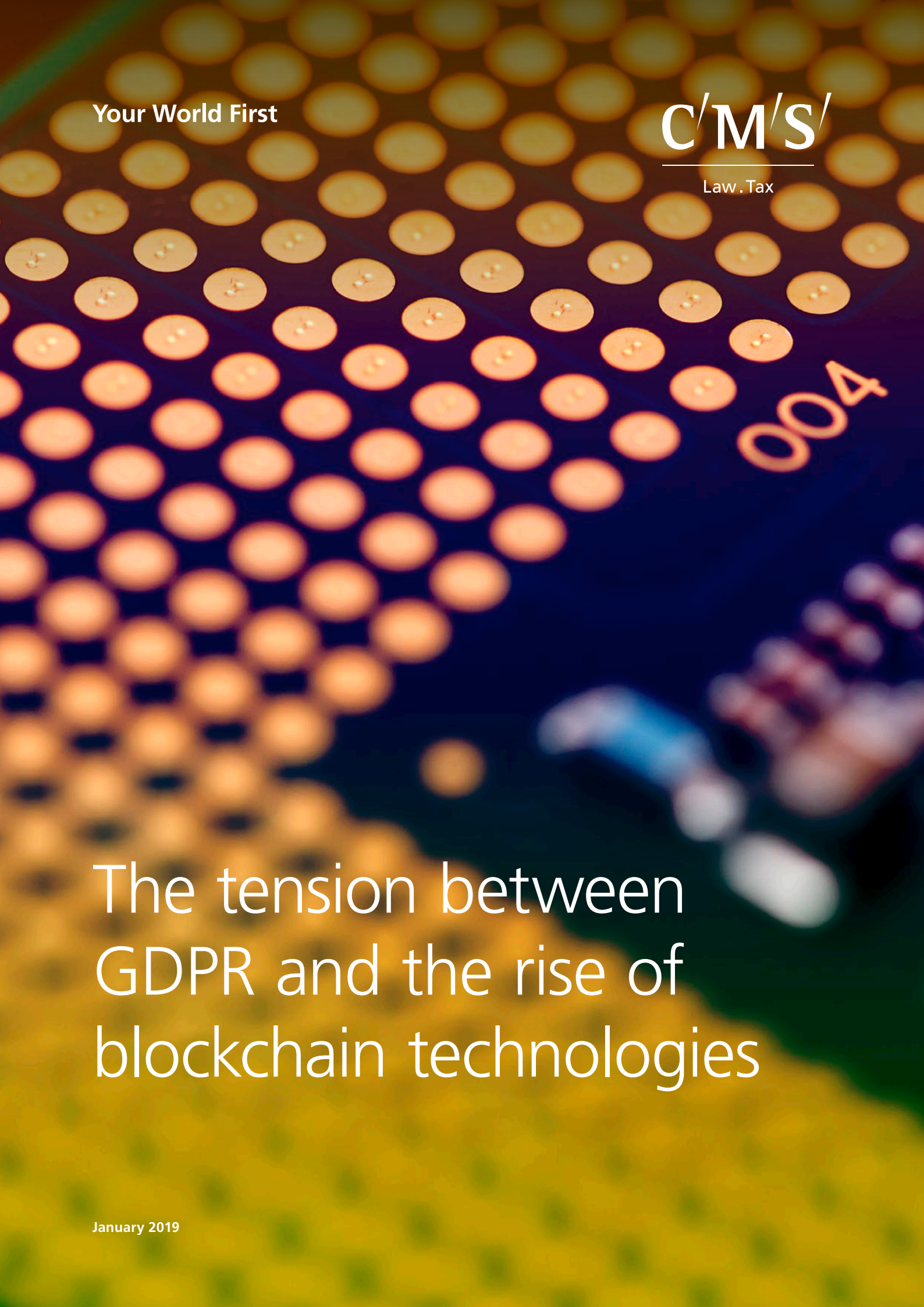
Your World First

C/M/S/

Law . Tax




# The tension between GDPR and the rise of blockchain technologies

January 2019

# Contents

# Introduction

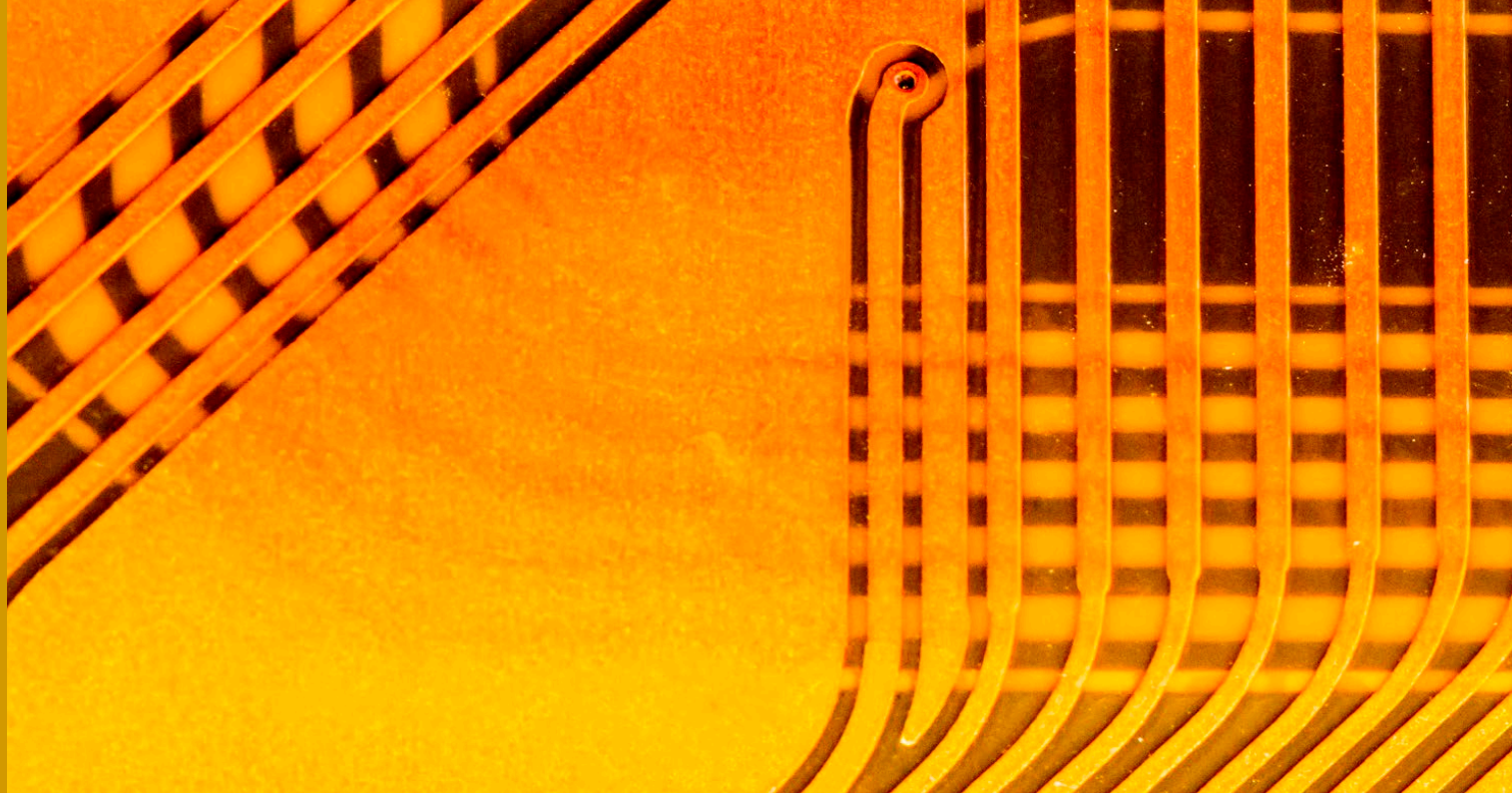
## The tension between GDPR and the rise of blockchain technologies.

We live in an era of rapid technological development. Though this provides humanity with amazing opportunities to enhance our standard of living, it also forces lawmakers to work around the clock to analyse and capture the implications of the technology into legislation. The same is true for the subject of this paper – the tension between the relatively new General Data Protection Regulation (GDPR) and the quick rise of blockchain and other distributed ledger technologies (DLTs). GDPR was drafted based on a world in which centralised and identifiable actors control personal data. Blockchain works radically differently. This technology aims to move the power over personal data away from centralised entities by processing it in a decentralised environment. One could imagine that the process of applying legislation based on a centralised view to technology without a clearly identifiable centralised entity might cause some tension. However, the decentralised nature of blockchain technology is not the only factor that causes legal and compliance challenges. The near immutability of transactions, of code (e.g., smart contracts) and, in general, of blocks in a blockchain potentially affects the rights of data subjects.

This paper briefly addresses three main issues arising out of the tension between the GDPR and blockchain. These are:

1. **Processing of personal data**. Encryption and hashing are often used for the obfuscation of data and are therefore fundamental to blockchain technology. The question of whether data qualifies as anonymous after it has been obfuscated by one of these techniques is being hotly debated at the moment.
2. **Identification and obligations of data controllers in a decentralised environment.** GDPR assumes there is always an identifiable entity that is responsible for determining the purpose and means of processing personal data. In a decentralised network, in which everyone can theoretically participate, this can prove problematic. This is especially difficult in the case of a public, permissionless blockchain.
3. **Exercise of key data subject rights.** Due to the nature of most current blockchain and other DLTs where data can only be appended, not altered, it is, for example, difficult to guarantee the right to be forgotten and the right to rectification.

Addressing these issues will be mainly relevant for public, permissionless blockchains, because they are most problematic from a GDPR point of view. In private environments, data is generally only accessible to members of a closed group. In the case of permissioned blockchain applications, a person must have been granted prior access to add data to the ledger. Private and/or permissioned environments give companies a lot more control and are less problematic from a data protection perspective. Before we dive deeper into these issues, it is worth noting that none of these issues have been conclusively settled by an authorised authority. Currently, there is no 'one size fits all' solution to make each and every blockchain GDPR-compliant. Rather, the question of whether a blockchain or other DLT solution is GDPR-compliant will need to be examined on a case-by-case basis.



# When does GDPR apply?

The GDPR only applies where personal data is being processed. Personal data is defined as any information relating, directly or indirectly, to a natural living person, whether the data identifies the person or makes him or her identifiable. Processing means any operation or set of operations performed on the data, such as collecting, recording, and altering the data. It is important to note that the GDPR also applies to controllers and processors established outside the European Union, where such controllers and processors process personal data in connection with offering services or goods to EU data subjects, or in respect of the monitoring of data subject behaviour within the EU.

### Do blockchains process personal data?

As a first step, let's see what kind of data is typically stored on blockchains:

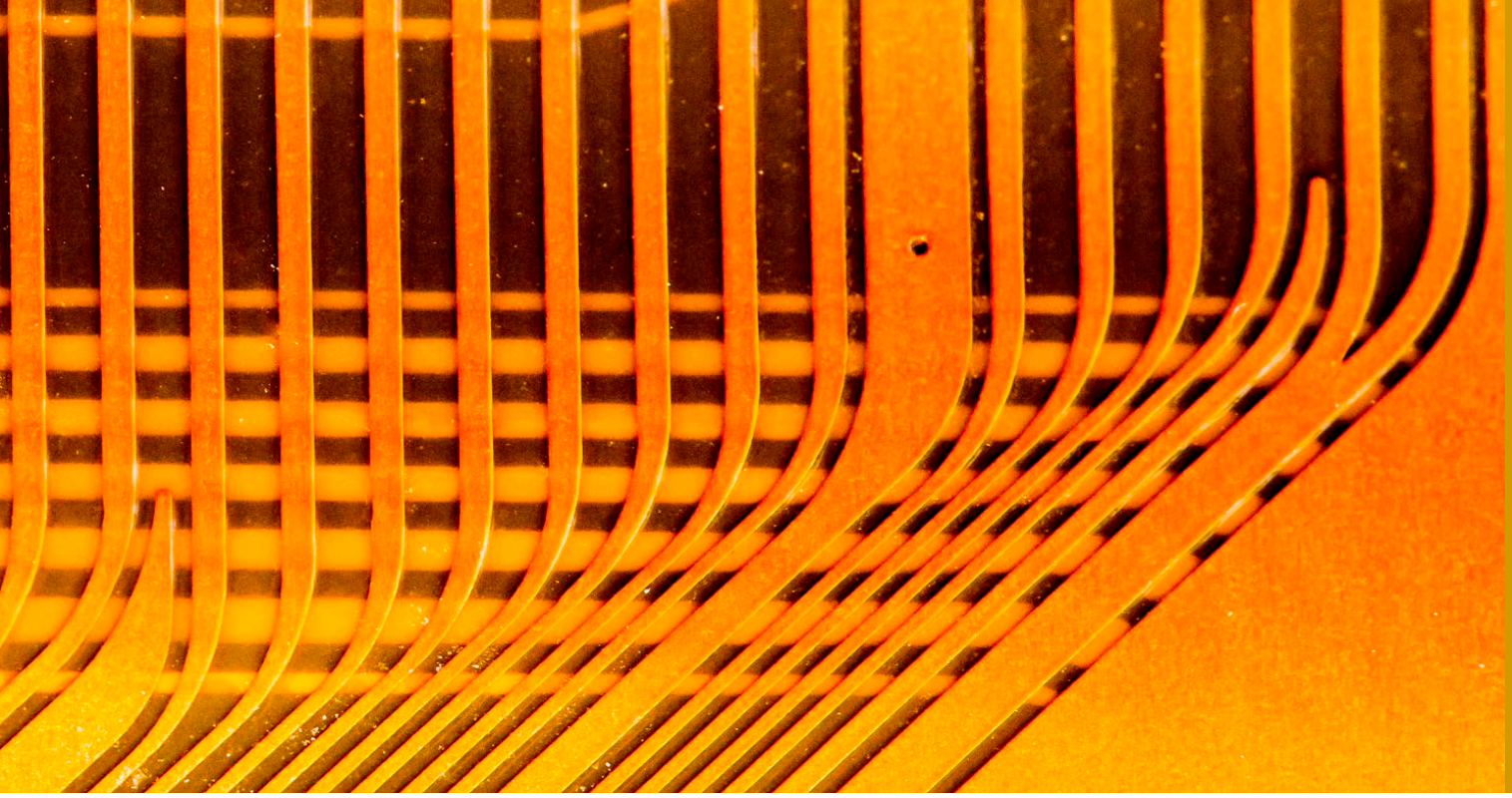
- **Transactional data**, which can be anything and depends on the purposes for which the blockchain technology is being used. This type of data can be stored on a blockchain in plain text, in encrypted form, or in hashed form.
- **Public keys**, which are pseudonymous identifiers of blockchain users. Here, the keys are encrypted and/or hashed and do not directly reveal the identities of the users. However, the GDPR also categorises identifiers and certain data (namely, that which can be used to single out individuals) as 'personal data,' which means that in certain cases, public keys may be classified as personal data where said keys can be linked to particular data subjects.

### The difference between pseudonymised and anonymised data

The Article 29 Working Party (now called the European Data Protection Board) is an important data protection group with representatives from each member state that inter alia provides guidance on the difference between pseudonymised and anonymised data. This distinction is important because, while pseudonymised data is considered personal data (and therefore is caught by GDPR), the GDPR does not apply to anonymised data. In their report, the Working Party states that anonymisation results from the processing of personal data to irreversibly prevent identification. To determine whether this is the case, account should be taken of all the means reasonably likely to be used to identify the person. The assessment must consider the cost, the time required and the technology available at the time of identification. This brings us to an important concept for establishing whether a blockchain solution is GDPR-compliant – the 'lifecycle' of data.

### The 'lifecycle' of data

We believe that the classification of data as either personal or anonymous is not as binary as it may appear. Throughout its 'lifecycle', data can be classified as either personal or anonymous at different points in time. By creatively storing data in an off-chain environment, and linking that data to a blockchain via some kind of lookup table, it is possible to capitalise on the transitory nature of data.



Let's say you have built a platform that allows people to rent out their cars to those in need of cars. In this case, the blockchain is used strictly as a payment channel and, after payment, a customer receives a unique car token with which to enter the car. For the platform to work, however, there has to be a link between the users' identities and their public keys. The details of their identities and the links can be kept in an environment where they can be modified and deleted (off-chain). To be extra safe you may even want to oblige parties to create unique public keys using your platform for each relationship. If you destroy the link that has been used as an identifier, all that is left on that blockchain is a public key and its transaction history. The public key is just a string of characters that, in itself, may or may not amount to personal data. Following deletion of the link, whether the data qualifies as either personal or anonymous depends on what is left on that blockchain and the likelihood of linkability. If all that is left is three simple transactions between two anonymous public keys, the ability to link that to an identifiable natural person may become practically impossible. Therefore, the data that was once considered personal in the GDPR sense, may have morphed into anonymous data.

This is an interesting way to guarantee data subjects the effective exercise of their rights (i.e., erasure and rectification). Whether this solution works must be assessed on a case-by-case basis.

### Is hashed personal data still considered personal data?

The simple answer to this question is 'yes' – though there appears to be some wiggle room according to various data protection authorities. However, we have already established that, under the GDPR, the threshold for anonymisation is high and can only result from obfuscation techniques that irreversibly prevent identification.

In general, hashing is considered a pseudonymisation technique. As pointed out by the Article 29 Working Party: 'if the range of input values the hash function are known they can be replayed through the hash function in order to derive the correct value for a particular record. For instance, if a dataset was pseudonymised by hashing the national identification number, then this can be derived simply by hashing all possible input values and comparing the result with those values in the dataset'.

Attackers could be warded off by using unique secret keys as additional inputs for each transaction. For example, a person could add the entire Harry Potter books collection into the hashing algorithm. This would make it a lot harder to derive the correct value for the record, as this would create a unique hash for each transaction.

In a report on blockchain technology the French data protection authority (CNIL) also cites hashing via the use of a secret key (as an additional input) as a possible solution in order to anonymise data. They reason that when the secret key is deleted, the proofing or verification of the information that has been hashed is no longer possible. In practice, the hash would no longer pose a risk to confidentiality. To reach this level of safety, the information would also need to be deleted on any other systems in which it has been stored for processing.

The question of whether hashed personal data still amounts to personal data for the purposes of GDPR is being hotly debated at the moment. The most desirable outcome would be that the answer depends on the infrastructure of the platform and the obfuscation techniques being used.

# Who is responsible for ensuring GDPR compliance?

Data controllers and processors are, to differing degrees, each responsible for ensuring compliance. The controller is the natural or legal person who determines the purpose and means of processing personal data, to whom data subjects turn to execute their rights, and who is ultimately accountable for compliance and is held liable if the rules are breached. A key word for GDPR is 'accountability', directed at (centralised) organisations and centralised data structures. By contrast, blockchain is focused on running decentralised databases without the need for trusted authorities or central servers.

### How to identify a data controller in a blockchain environment

Depending on the exact infrastructure it can be difficult to identify the data controller in a blockchain ecosystem. In a private, permissioned blockchain environment, controllers are relatively easy to identify. However, in a public, permissionless environment, this can prove very difficult. The following list identifies the potential 'suspects' eligible to be designated as potential data controllers in a public, permissionless blockchain.

— **Protocol developers**: in our view, it is not likely to qualify protocol developers as data controllers and not desirable to qualify protocol developers as data controllers in a blockchain environment. First, because they do not (usually) process personal data when developing a protocol and also do not prescribe or decide on a purpose for the use of said data, or how to deal with same. Though they create the protocol, the algorithms, and the software, they do not determine the purpose for which this solution or protocol is used. Second, holding the creator responsible for everything that happens on a blockchain, would be the same as holding the creator of the internet responsible for everything that happens on the world wide web. This is simply not feasible and is certainly not desirable.

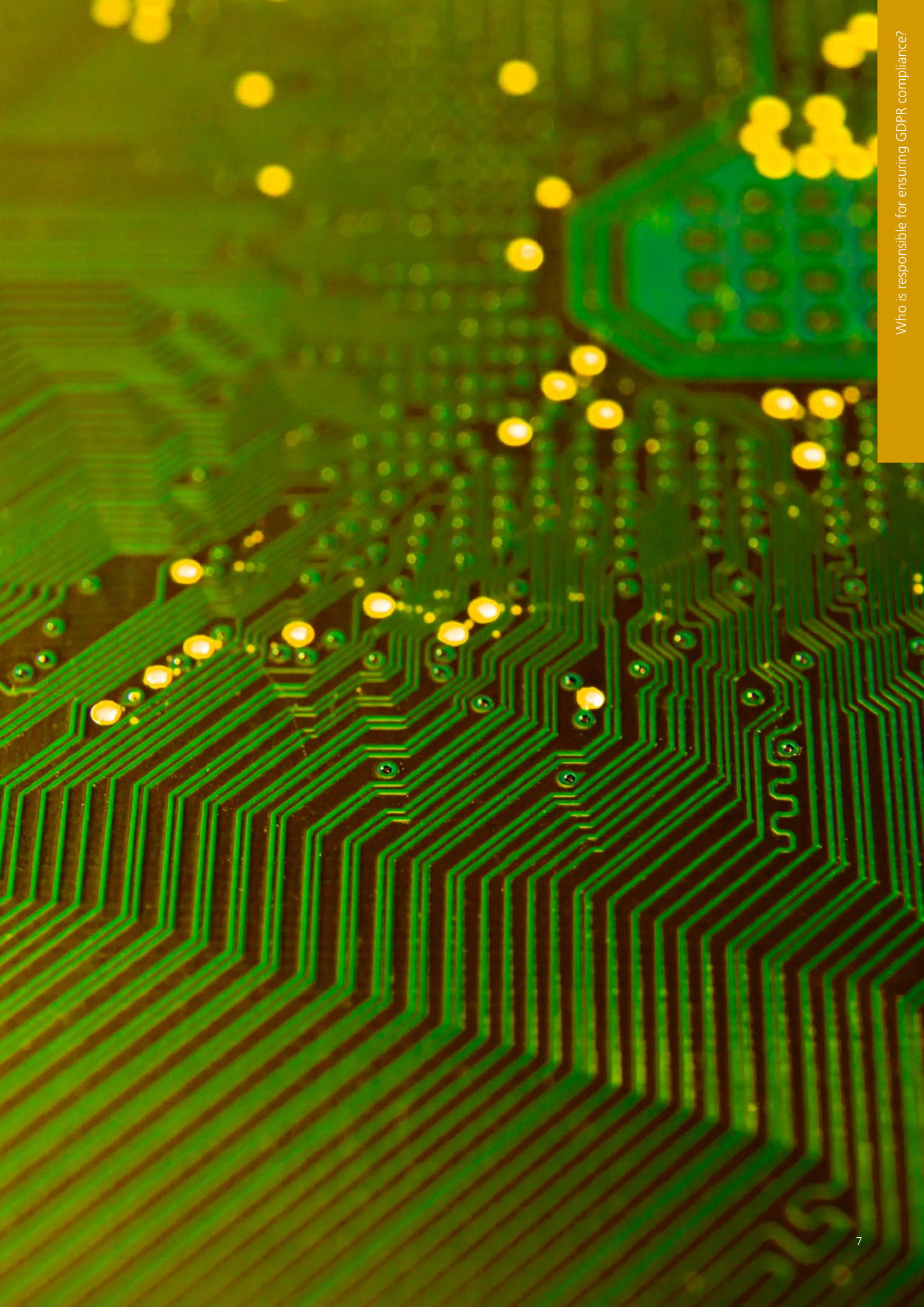
— **Validating nodes**: they run the protocol, and are allowed to add data to the ledger and store a copy of the ledger. They are also not likely to be classified as data controllers, as they do not define the purpose and means of the processing. This last part is sometimes debated because validating nodes are free to choose which version of the protocol they use and thus according to which rules the protocol works. The qualification of validating nodes as processors is also undesirable due to the obligation on data controllers to contract with each and every processor (and thus node) in the network.

— **Network users**: they are people who sign and submit transactions to the network. They can either be legal entities or natural persons, and can qualify as controllers. These activities could in theory fall under the household exemption of the GDPR, which, if applicable, means that GDPR will not apply. However, as confirmed by the Article 29 Working Party and later repeatedly confirmed by the Court of Justice of the European Union (e.g. cases Lindqvist, Satamedia, and Jehovah's Witnesses), the exemption does not apply when data is submitted to an undetermined number of persons – as often happens in the context of public, permissionless blockchains.

Some voices within the relevant literature on the topic have considered nodes and network users to be either controllers or joint controllers. Whether the interactions of participants in decentralised networks are classified as separate or joint (or whether there is no responsibility whatsoever) should be assessed on a case-by-case basis.

### Further questions

As shown above, the identification of a data controller in a public, permissionless blockchain can be challenging. The question that arises is: what if nobody qualifies as the data controller in a given relationship, and is it possible to have no controller at all? Does the GDPR apply at all in that situation? A very interesting possible solution would be for regulators to come up with standards/minimum requirements that can then be translated into code and implemented into a blockchain's protocol in order to foster GDPR compliance from the beginning. This would be highly appreciated within the blockchain community since it would alleviate some legal uncertainty.



# Does blockchain hinder the exercise of some data subject rights?

Most data subject rights are not problematic at all in a blockchain environment. Things can get complicated, however, in certain circumstances – for example, in respect of the right to erasure and the right to rectification. Both rights could be guaranteed by creatively making use of off-chain solutions, in which case no personal data would be stored on a public blockchain. The right to rectification could be exercised by adding a new block with rectified data to the chain, without deleting the block containing the incorrect personal data, although there is no court precedent or any official guideline on whether this solution meets the requirements of the GDPR. The same applies to another solution which would involve creating unique hashes for each piece of data by using an additional secret key – in their report the CNIL also argues that this allows data subjects to get closer to the effective exercise of their rights. Neither solution results in the erasure of the data in the strictest sense of the word but might in some cases anonymise the data. Please note that this has not been conclusively settled by any authorised authority. Another difficulty is that according to the GDPR, the data controller must inform each recipient of the persons to whom their personal data have been disclosed – which is technically and practically impossible. The GDPR exemption 'if this provides impossible or involves disproportionate effort' may be applied in this situation. Additionally, the exercise of the right of data portability in blockchain technology could also be a challenge, because copying the data in a user-friendly format is a challenge for blockchain applications.

**Does the use of blockchain per se require the controller to carry out a Data Protection Impact Assessment (DPIA)?**

On the basis of the GDPR, the data controller must carry out a DPIA if the data processing is likely to be a high-risk for the rights and freedoms of data subjects. Implementing state-of-the-art or new technologies does not, in itself, make the DPIA mandatory and therefore using a blockchain does not make a DPIA mandatory per se. A DPIA is only required if there are other data processing circumstances which, when coupled with new technologies, result in a high risk for data subjects. In their DPIA guidelines, the Article 29 Working Party states that a DPIA is obligatory if the data processing in itself prevents data subjects from exercising their rights under the GDPR. This could, for example, be the case in a blockchain environment wherein public keys are deemed to be pseudonymous data. The fact that a DPIA is obligatory in the event that data subjects are prevented from exercising their rights seems to imply that even then, GDPR compliance is not impossible if appropriate technical and organisational measures are implemented. It is also notable that carrying out a DPIA is (only) an obligation of controllers.

# How can data protection principles be fulfilled within blockchains?

Data Protection by Design exclusively applies to controllers and (only) encourages them to take the right to data protection into account when developing, designing, selecting and using tools for processing personal data (recital 78). Data Protection by Design does on its own not constitute an obligation on controllers of data processing in blockchains, but rather highlights the importance of fulfilling the data protection principles of Art. 5 GDPR as soon as personal data is processed.

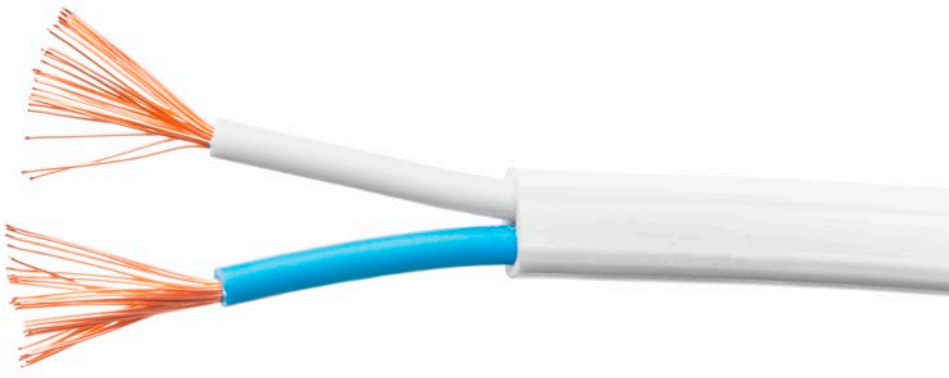
The two main features of public, permissionless blockchains usually are:

1. Data stored on the ledger is generally accessible; and
2. Data cannot be easily removed from the ledger.

In these blockchain environments the onus of compliance can be put on the users by making them agree on certain terms of use before they are granted access. These terms could prohibit adding certain kinds of personal data or require users to obtain consent or other legal bases for processing, and could therefore ensure compliance with the lawfulness and transparency principle of GDPR. Data minimisation is challenging for blockchain-based data processing, because once data is added to the chain, it will remain part of that blockchain in perpetuity. Therefore, off-chain storage of transactional personal data can aid with blockchain compliance issues. Lastly, GDPR obliges the data controller to implement appropriate technical and organisational measures – like pseudonymisation, encryption – to ensure the safety of data. Off-chain transactional data storage is a good solution, but for public keys blockchain developers should adopt necessary risk-management solutions.

## Concluding remarks

It is hard to align blockchain technology and the GDPR, but it is certainly not impossible. When developing your blockchain solution, always remember to take into account data protection principles and data subject rights, and enable users to agree to certain terms of use or governance rules for the platform. Document the measures you have taken in terms of obfuscation, off-chain storage etc., and also add the advantages your blockchain solution has for the right to the protection of user data. Make sure to only store personal data on a blockchain if it is strictly necessary and try to keep as much as possible in an off-chain environment.



# How CMS can help

The challenges arising from data are countless and inescapable in our maturing technological landscape. To future-proof your organisation, and unlock opportunity from your data, you need alert and experienced lawyers who'll deliver practical advice. CMS has over 100 data protection and technology sector-focused lawyers ready to deliver legal and practical advice. They are at the forefront of advancements in technology law, including issues related blockchain and other distributed ledger technologies.

## One-stop-shop

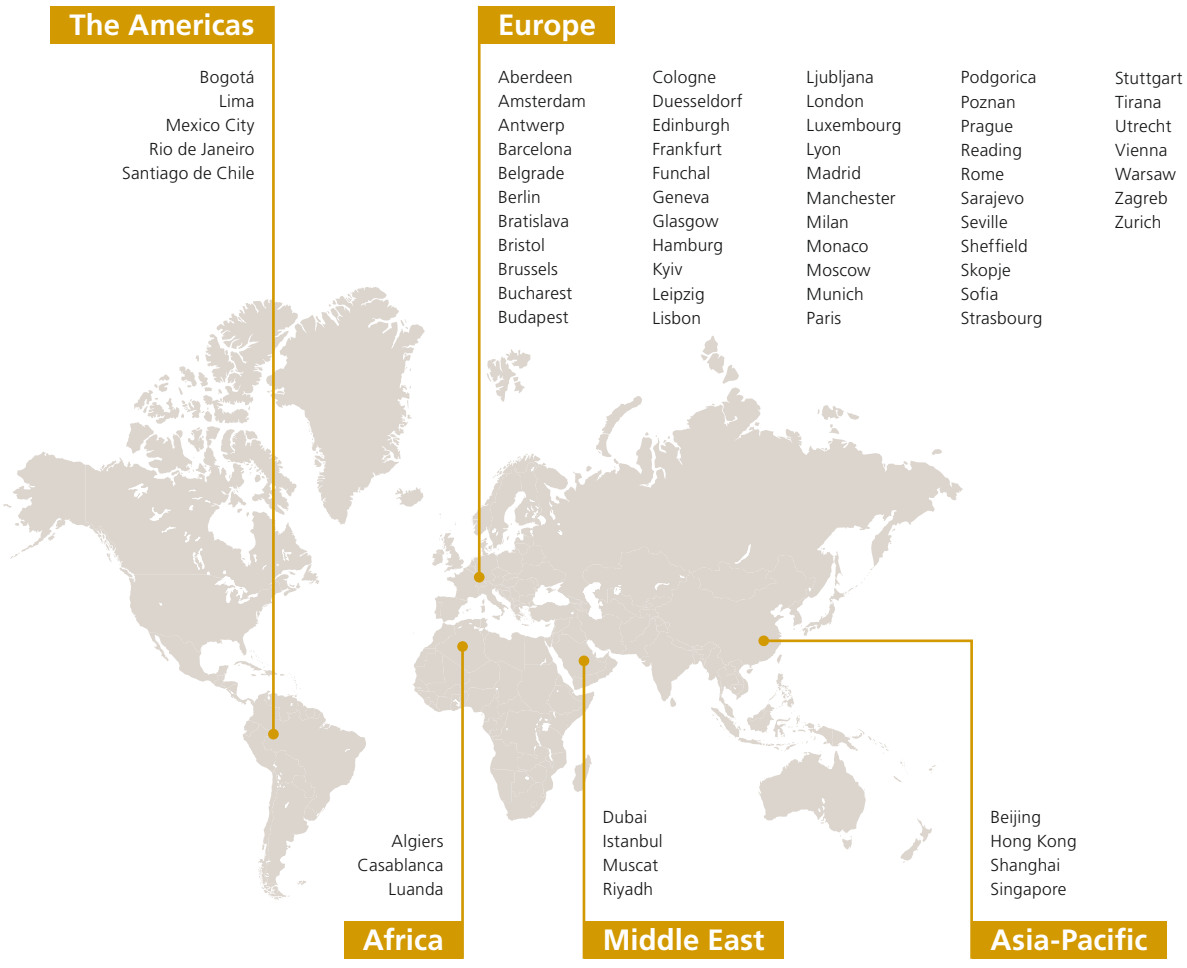
Clients turn to CMS to advise on global data privacy, protection and information security projects. Leading multinational companies, many of which hold large amounts of sensitive data and are heavily regulated, have instructed us to advise them on multi-jurisdictional data privacy and information security projects.

## Global AND local

Our teams are flexible in that they handle both large multinational projects but can also deep-dive for niche, country-specific advice. The teams are on the ground in over 40 countries, speak the local language and understand the local laws – but crucially in a global context.

## Pragmatism and business acumen

CMS has a knack for turning legal advice into practical solutions that make sense not just to your legal teams, but to your other employees, such as the HR function, or software engineers.



## Selected experience

**Various start-ups and mid-sized companies**

Advising on financial, tax and civil law aspects of the sale of Currency, Utility and Security Tokens (ICOs, STOs).

**Berlin based blockchain company**

Advising on the use of blockchain in the context of artificial intelligence (AI), with a focus on data privacy.

**Various start-ups and mid-sized companies**

Advising on data privacy and civil law aspects of the development and implementation of blockchain solutions.

**European energy trading network**

Advising on data privacy, liability, contract drafting issues resulting from using blockchain technology.

**Supply chain consortium**

Advising on founding a company suitable for Blockchain projects, including the contractual and regulatory framework.

**Advising a global energy supermajor**

Advising on an innovative use of blockchain in a prosumer project.

**Korean life sciences and healthcare services provider**

Advising on the legality of an ICO in Singapore by a healthcare data platform that will allow individuals to own and trade their own healthcare data.

**Major energy company**

Advising on its proposed peer to peer electricity trading platform utilising blockchain technology in the UK, including advice in relation to electricity regulatory issues and interface with the regulator.

**DAX 30 company**

Advising on financial and tax aspects of a multi-jurisdictional sale of Security Tokens (STO).

**Global bank**

Advising on data protection and e-privacy issues in connection with an innovative platform that combines B2B and banking functions in Eastern Europe.

**Global consumer goods manufacturer**

Advising a global review of its data protection and information security policies, processes and practices in preparedness for the GDPR, covering over 50 jurisdictions.

**A global online retailer**

Advising on various day-to-day data protection issues, including notification and registration obligations, international data transfers and data subject access requests.

## Contact us


**Dr. Markus Kaulartz**
Senior Associate, Technology, Media and Communications
**T** +49 89 23807 305
**E** markus.kaulartz@cms-cmno.com

**Katja van Kranenburg-Hanspians**
Partner, Head of Technology, Media and Communications, The Netherlands
**T** +31 20 301 64 02
**E** katja.vankranenburg@cms-dsb.com

**Michael Kamps**
Partner, Global Co-Head of Data Protection
**T** +49 221 7716 139
**E** michael.kamps@cms-hs.com

**Christian Runte**
Partner, Global Co-Head of Data Protection
**T** +49 89 23807 304
**E** christian.runte@cms-hs.com