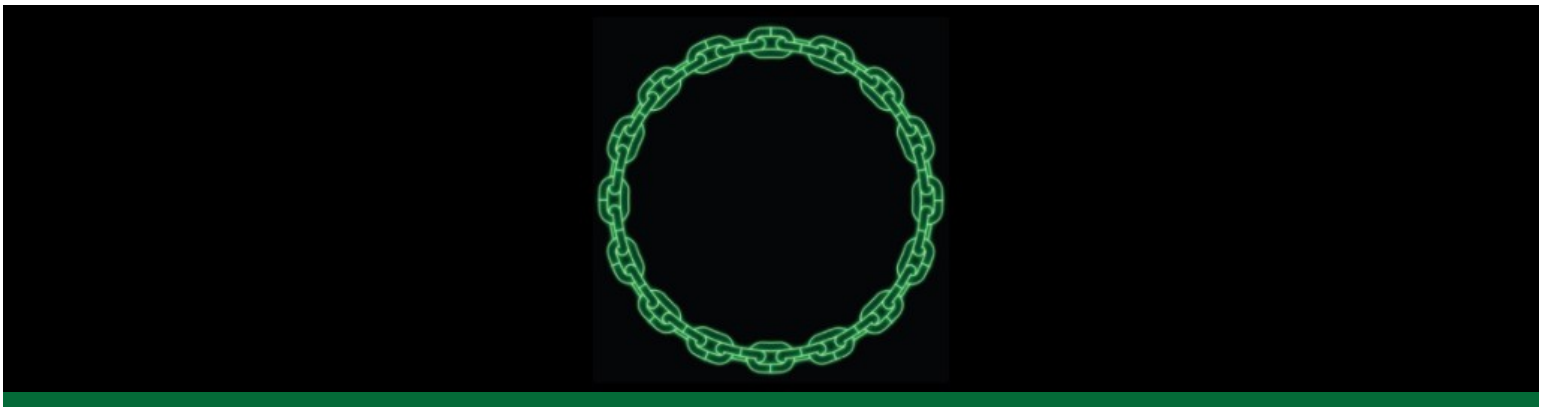
Deloitte.



Insights

Blockchain from a perspective of data protection law

A brief introduction to data protection ramifications

While blockchain applications may provide for an appropriate means of implementing the principle of “privacy by design”, the extent to which such technology may be deployed will be limited by the rights granted to individuals under the European General Data Protection Regulation.

Blockchain applications are currently amongst the most discussed topics when it comes to the precursors of the fourth industrial revolution. Within the global Deloitte network, the Deloitte Blockchain Institute was founded in order to analyze and consult on the technical and economic potentials and risks of blockchain applications for sector-specific industries (e.g. telecommunications or media).

The following article deals with blockchain applications from the perspective of

data protection law, in particular the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation - "**GDPR**"), which will enter into force in May 2018. In addition to an approximation to the term blockchain (cf. section I.), the main question addressed by this article is, to what extent this technology will impact on those areas of life that have been traditionally regulated by analogue law and institutions (cf. section II.). Finally, the potential of blockchain is briefly addressed as an instrument of data protection (cf. section III.) and explains the extent to which data protection law may create certain boundaries to potential applications of blockchain technology (cf. section IV.).

I. Blockchain: a brief introduction

As the term already suggests, one of the essential characteristics of a blockchain is the concatenation of blocks. More specifically, such blocks are comprised of a certain number of cumulative records, the contents of which are interconnected in such manner that each subsequent block contains a cryptographic image of the previous block. Thus it can be ensured that data cannot be manipulated unrecognized after the respective data has been entered into a block, completed and "attached" to a subsequent block. New blocks are always created in a so called “consensus procedure” that ensures the integrity of the data content to be included in each of these blocks.

From a perspective of functionality, the blockchain may therefore be described as an electronic database particularly secured against data manipulation.

Originally, the blockchain was conceived as an approach within the digital (crypto) currency system *Bitcoin* in order to solve the problem of so-called *Double Spending* occurring in distributed networks. However, its potential scope of application is not limited to virtual currencies. To the contrary, blockchain-based databases may be deployed in all other application scenarios in which the advantages of a distributed network (e.g. high-grade redundancy due to, inter alia, absence of a single point of failure), but at the same time it remains crucial to warrant the integrity of the data contained therein. In this context, apart from numerous applications in the financial sector, such applications may encompass the trade of digital, copyrighted works such as music or video files via internet, or the digitization of registries equipped with public credence, such as the land register (respective projects run in Sweden and ran in Honduras respectively) and commercial registers. In the United Kingdom, the feasibility of a blockchain-based administration of social services has been researched recently as well.

II. Blockchain as a surrogate of legal regulation

While the above-mentioned possibilities of use are limited to mere tasks of documentation and file management, blockchains also proof useful in order to increase the trustworthiness and thus the transportability of so-called *smart contracts*. Essentially, these are computer protocols which, by implementing an "if-then" sequence at the level of machine code, simulate the logic of a contract and ultimately enable contracts to be "self-completing" (i.e. computer-implemented without further human intervention). *Smart contracts* are already interesting for a variety of application fields where reduction of transaction costs (keyword micro payments) and / or lowering of performance risks (e.g. standardized mass contracts) is of importance. Another obvious scenario in which blockchain-based smart contracts could proof most useful are online

alternative dispute resolution procedures as those already commonly used by providers of online market platforms today. On the advent of the Internet of (autonomous) things (*IoT*) at the latest, however, finding ways to automate the conclusion and execution of contracts will become an inevitable prerequisite in order to enable the handling of the mass of *M2M*-interactions to be expected. In both of the afore-said scenarios, blockchain databases may provide for reliable information upon which the algorithms underlying a given *smart contract* may decide, as to whether the conditions defined in the (contract) program code are realized.

III. Blockchain as a catalyst for data protection

From a data protection perspective, blockchain databases are particularly interesting because they allow - at least in theory - transactions between parties without having to disclose their identity directly to the contracting party or the public. Anonymity and pseudonymity are also addressed as data protection law instruments. If a transaction cannot be traced back to the involved individuals, their fundamental right to self-determination is not affected. As the scope of European data protection law is not established for such mere (transaction) data (see also recital 26 GDPR), companies are legally permitted to use and process such data without being subject to specific data protection restrictions.

The popular crypto-currency *Bitcoin* is often referred to as one example of a blockchain database with potential for data protection, since *Bitcoins* provided for an "anonymous, non-persecutable" means of payment. However, it has more and more become clear that such generalized statements will most likely not hold true. Paradoxically, one reason for this problem lies in the one property of the blockchain that enables the anonymity of its user to the public, this is to document all transactions publicly and in a tamper-proof manner. Whereas it is true that no names, addresses, telephone numbers, or any other comparable information making it possible to readily identify the participants without significant effort are captured in the corresponding transaction data entries of the blockchain, there are various possibilities remaining for the de-anonymization of corresponding entries. For example, one study has shown that the *Bitcoin* address of a service user documented in the blockchain can be traced back to its IP address, which in turn can be traced back to a specific internet connection or connection owner. Another research paper could prove that a user- and transaction-network may be created on the basis of the publicly accessible blockchain entries to the *Bitcoin Ledger*, with the help of which the allegedly anonymous transactions may be traced back to certain users.

It remains important to note, however, that the above-mentioned attack areas for de-anonymization are not system-inherent, that is, could be avoided to a certain extent if the technical design was respectively adapted. To this extent, companies considering the utilization of blockchain technology should bear in mind the principle of data protection (*privacy by design*), which is now standardized in Article 25 GDPR, when it comes to the the conception of blockchain databases and applications in order to ensure their business model's legal compliance. How far blockchain databases are suitable for the implementation of the seven basic principles of privacy by design remains to be seen in practice: while some of these principles (e.g. transparency, privacy by default, data protection as integral part of application design) may be directly implemented into the technological layer of blockchain applications, the feasibility of other principles, in particular the effectiveness of data protection throughout the entire life cycle of the application, may turn out to be not readily achievable. The extent to which companies need to use technical measures to meet their obligations under Article 25 GDPR is currently largely unresolved. To this extent, the legal text only provides an abstract contextual, risk, cost and

individual assessment criterion. To this extent, there seems to be a broad consensus in Germany between industry stakeholders, regulators and civil society to jointly and rapidly drive the development of interoperable standards within the meaning of Article 25 GDPR.

Finally, in order to illustrate the extent to which blockchain databases could be used for the purposes of data protection, a concrete application example may be found in the purpose limitation principle set out in Article 25 GDPR. According to this principle, personal data may only be collected for clear and legitimate purposes and not be further processed in a manner incompatible with these purposes (see Article 5 (1) (b) GDPR). One way of monitoring compliance of electronic data processing with the purpose limitation principle is to provide individual personal data with a meta-tag, that is unique and durable electronic labels that provide information on the nature and extent of the processing allowed for the personal date each concerned. A decentralized register managed as a blockchain could be used here to make the processing of personal data by companies more transparent and to ensure the efficient sanctioning of possible infringements.

IV. Potential conflicts with data protection law

The inherently tamper-proofness of blockchain databases is, from a data protection point of view, despite its potential for application as a means of enabling data protection by design, also a potential threat to the individual rights of data protection and privacy held by EU citizen.

In May 2014, the European Court of Justice ruled that citizens of the EU were entitled to a claim against internet search engine operators to remove any content retrievable from the index of search results, as far as such referred to information on the individual concerned that was of no particular significance for the public interest. From this right to be "de-indexed", the European legislator derived a more general “right to be forgotten" enforceable against any data controller and now being legally anchored in Article 17 GDPR. Given the fact that certain application scenarios (for instance a legally binding marriage) inevitably require personal data to be documented in the ledger, it becomes clear that concerned service providers might face severe difficulties to fulfill respective claims of their customers. In the end, it comes down to the question if such service providers may be obligated, possibly accepting the destruction of the data integrity of the entire database, to delete or correct data entries having become obsolete in the meantime.

Against this background, the development of and research on blockchain mechanisms remaining subsequently editable appears to be of paramount significance. Prototypes bearing such feature have already been developed in line with the needs of large banks, however, they come with a significant limitation: the subsequent editable ability of data records while maintaining their authenticity requires nomination of trustworthy administrators authorized to alter the blockchain’s ledger according to a predefined rule set. Some of the essential characteristics of the blockchain in its implementation form as decentralized peer-to-peer database may thus not be retained.

At the same time, it is clear from this example that companies engaging in use of blockchain technology will have to deal with the relevant regulatory framework, including data protection law, at an early stage in the development of any blockchain-based application, and must ensure that its specific technical design meets the requirements set out by the applicable laws.

Your Contact

Stefan Wilke
Counsel
stwilke@deloitte.de | 0211 8772 3402

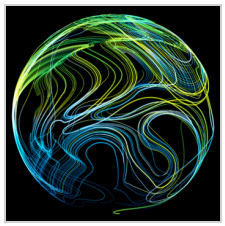
Stefan Wilke has joined Deloitte Legal in 2009. Before, he worked as an inhouse counsel of a leading internationally acting listed laboratory and process technology provider in the fields of biotechno... More

Recommendations

Deloitte Legal

About Deloitte Legal

Representing tomorrow



Review 2016 and prospects for 2017

These have been and will be the legal topics in the areas of privacy and IT security

IP Newsletter

Current Jurisprudence and Developments in the field of Intellectual Property (IP)

Related topics

- Legal
- Blockchain
- Media
- Telecommunications

Contact Deloitte Legal	Vacant Positions Deloitte Legal	Submit RFP Deloitte Legal

https://www.facebook.com/Deloitte.Deutschland

https://twitter.com/DeloitteDE

https://www.linkedin.com/company/deloitte-deutschland

http://www.youtube.com/user/DeloitteDeutschland

https://www.xing.com/company/deloitte

https://www.instagram.com/deloittedeutschlandkarriere/

https://plus.google.com/+DeloitteDeutschland