BRIEFING

STOA Options Brief

European Parliament

Blockchain and the General Data Protection Regulation

Can distributed ledgers be squared with European data protection law?

This briefing is based on a STOA study that examined the relationship between blockchain technology and European data protection law. The study showed, first, that there is significant tension between the very nature of blockchain technology and the overall structure of the General Data Protection Regulation (GDPR). Whether specific blockchain use cases are compliant with the supranational legal framework can, however, not be examined in a generalised fashion but is best determined on a case-by-case basis. Second, the study also highlighted that in specific cases this class of distributed technologies may offer distinct advantages that can be helpful in achieving some of the GDPR's objectives. It is on the basis of the preceding analysis that the study developed concrete policy options that could be adopted to ensure that distributed technologies develop in in line with the objectives of the legal framework.

Policy option 1: regulatory guidance

The key point highlighted in the first and main part of the study is that there is currently a lack of legal certainty as to how various elements of European data protection law ought to be applied to blockchain. This uncertainty is anchored in two overarching factors. First, it has been seen that very often the very technical structure of blockchain technology as well as its governance arrangements stand in contrast with legal requirements. Second, it has also been observed that trying to map the regulation to blockchain technologies reveals broader uncertainties regarding the interpretation and application of this legal framework. The GDPR is legislation that is based on broad general principles. This brings flexibility and adaptability advantages in an age of fast technological change, but also has downsides, at times for instance making it difficult determine with certainty how a specific provision ought to be applied in a specific context.

Indeed, one year after the GDPR became binding and although the legal regime is largely based on the previous 1995 Data Protection Directive, it is evident that many pivotal concepts remain unclear. Many instances of that phenomenon have been highlighted above. For example, it is currently unclear where the dividing line is between anonymous data and personal data, owing to conflicting statements to this effect in the regulation and in the Article 29 Working Party's interpretation. Moreover, whereas the GDPR recognises a right to 'erasure' that data subjects are free to exercise in some circumstances, there is no indication of what 'erasure' actually requires. As such, it is unclear whether erasure in the common-sense understanding of the word is required or whether alternative technical approaches with a similar outcome may be sufficient. These are important questions as erasure in the common-sense understanding of the word is difficult to achieve in distributed ledger technology (DLT) whereas alternative technical approaches have been envisaged. Oftentimes, the interpretation of core GDPR concepts is burdened by a lack of harmonious interpretations between the various supervisory authorities in the European Union.

Furthermore, in the blockchain context and beyond, there is an on-going debate regarding the allocation of responsibility for GDPR compliance. The regulation considers that the data controller is the entity determining the purposes and means of personal data processing. Yet, in practice only the purposes are taken into account to make that determination. This has led to an expanding number of actors that may be qualified as data controllers – particularly joint-controllers, as is also obvious from recent case law of the Court of Justice of the European Union (CJEU). In addition, there is a lack of legal certainty as to what consequences flow from a finding of controllership, precisely whether the (joint-) controller ought to comply with all GDPR requirements, only those assigned to it in an agreement with other joint-controllers, or only those that are effectively within its responsibilities, powers and capabilities. It is hoped that future case law, especially the upcoming judgment in *FashionID*, will clarify at least some of these questions, which are important for blockchain but also beyond.

The study has furthermore observed that blockchain technologies challenge core assumptions of European data protection law, such as that of data minimisation and purpose limitation. At the same time, however, this is a broader phenomenon, as these principles are also hard to map to other elements of the contemporary data economy, such as big data analytics facilitated by artificial intelligence techniques involving machine learning or deep learning. Indeed, the interpretation to be given to the overarching requirements of data minimisation and purpose limitation is not obvious in such contexts.

Whereas some have called for a revision of the GDPR, it is not clear that this is necessary. The regulation was designed as a form of principles-based regulation that is technologically neutral and should stand the test of time in a fast-changing data-driven economy. Thus, it is not the structure of the GDPR as such that causes confusion, rather the lack of certainty as to how specific concepts should be interpreted. This could be addressed through regulatory guidance without the need for legislative reform, which would itself come with significant limitations and disadvantages.

Regulatory guidance could as a matter of fact provide much legal certainty compared to the current status quo. This could take the form of various regulatory initiatives. On the one hand, supervisory authorities could coordinate through the European Data Protection Board (EDPB) to draft specific guidance on the application of the GDPR to blockchain technologies at supranational level, preventing the risk of fragmentation that would result from numerous independent initiatives in the various Member States. Whereas such specific guidance would be important to generate more legal certainty, revision of other, more general, guidance documents of the Article 29 Working Party would also be helpful. Indeed, it has been observed above that these have sometimes themselves generated uncertainty as to how specific provisions of the GDPR should be applied. It has, for instance, been seen that whereas the GDPR itself adopts a risk-based approach to anonymisation, the Article 29 Working Party has endorsed a somewhat divergent test. Updating some of these more general guidance documents, in particular those that have not been endorsed by the EDPB would help to address outstanding questions in the context of blockchain technologies but also beyond.

The provision of regulatory guidance would achieve a dual objective. First it would provide greater certainty for stakeholders in the blockchain space, who have long stressed that the difficulty of designing compliant blockchain use cases relates in part to the lack of legal certainty of what exactly is required to design a compliant product. Second, regulatory guidance on how the GDPR applies to blockchain, as well as on specific elements of the GDPR that have been the source of confusion more generally, could add more certainty and transparency in the wider data economy.

Policy option 2: support codes of conduct and certification mechanisms

As a technologically-neutral legal framework, the GDPR was designed in such a manner as to enable its application to any technology. This design presents many advantages, such as that it is supposed to stand the test of time and that it does not discriminate between particular technologies or use examples thereof. Indeed, as a principles-based regulation, European data protection law devises a number of general overarching principles that must then be applied to the specificities of concrete personal data processing operations.

The technology-neutrality of the GDPR however also means that it can at times be difficult to apply its obligations to specific cases of personal data processing, as evidenced by the analysis above. It is important to note that the regulation itself provides mechanisms specifically designed to deal with this: certification mechanisms and codes of conducts. These tools were included in the regulation specifically to enable the application of the GDPR's overarching principles to concrete contexts where personal data is processed. In contrast to the adoption of regulatory guidance as suggested above, certification mechanisms and codes of conducts exemplify a co-regulatory spirit whereby regulators and the private sector collaborate to devise principles designed to ensure that the principles of European data protection law are respected where personal data is processed. This has, for instance, been achieved in relation to cloud computing, where many of the difficult questions examined above also arose when these solutions were first deployed. The EU Cloud Code of Conduct was defined between the major cloud-computing providers as a means of securing GDPR compliance in collaboration with the European Commission and the Article 29 Working Party. Like blockchain, cloud computing has raised many difficult questions regarding GDPR compliance and the code of conduct was seen as one way to introduce more legal certainty in this area and secure greater adherence to the objectives of the regulation. As such, the establishment of codes of conduct and certification mechanisms could also be very useful in the context of blockchain technologies. This could, for instance, include the design of binding network rules regarding international data transfers.

Article 40 GDPR provides for the establishment of codes of conduct by associations and other bodies that represent categories of data controllers or processors. Article 42 GDPR moreover allows for data protection certification mechanisms to be established in the form of data protection seals and marks to demonstrate compliance with the GDPR. The notion of the certification mechanism is not defined although the reference to 'data protection seals and marks' would indicate that this could take the form of a trustmark visible through the user interface or similar mechanisms. Companies that are using DLT in their operations should accordingly be encouraged to develop codes of conduct and certification mechanisms specifically tailored to DLT. Whereas these initiatives do not remove the need for a case-by-case compliance assessment, they are valuable starting points for such an analysis. Moreover, codes of conduct and certification mechanisms are valuable steps towards ensuring that technical systems are designed to be compliant-by-design in line with the data protection by design and data protection by default obligations enshrined in the regulation.

Stakeholders relying on approved codes of conduct under Article 40 GDPR or certification mechanisms under Article 42 GDPR, moreover, benefit from a risk-management perspective. As a matter of fact, adherence to these standards can be used by the data controller to demonstrate compliance with its obligations under Article 24 GDPR. The European Union could, accordingly, encourage the initiation of related procedures that are complementary to the provision of regulatory guidance in order to resolve some of the uncertainties in this area.

Policy option 3: research funding

Regulatory guidance, as well as codes of conduct and certification mechanisms, could add much legal certainty where the tension between the GDPR and blockchain technologies stems from a lack of legal certainty as to how specific provisions of the GDPR ought to be applied.

This, however, will not always be sufficient to enable compliance of a specific distributed ledger use case with European data protection law. Indeed, it has been amply underlined in the above analysis that in some cases there are technical limitations to compliance. In such instances, regulatory guidance, certification mechanisms and codes of conduct may not go far enough to resolve a lack of compliance. In other cases, the current governance design of blockchain use cases stands in the way of compliance. These technical and governance limitations could be addressed by interdisciplinary research into these matters.

Such interdisciplinary research could, for example, define governance mechanisms that enable various controllers in decentralised networks to coordinate effectively in order to enforce data subject rights, something that, as has been seen above, is not straightforward in the current state of affairs – in DLT or elsewhere. Other interesting topics would include the design of mechanisms that enable the effective revocation of consent in contexts of automated personal data processing, as well as the definition of technical solutions to comply with Article 17 GDPR. More broadly, such research could also focus on data protection by design solutions under Article 25 GDPR; for instance the development of protocols that would be compliant by design.

This would benefit the development of compliant blockchain solutions in the European Union and, more broadly, could also serve to design solutions, for instance, for anonymity and data-sharing that would be of much broader relevance to the digital single market as they could also be deployed in other contexts. As data-ecosystems are increasingly decentralised even beyond the DLT realm, such research could benefit the digital domain more generally. This would benefit the digital single market, support the EU's global leadership role in data protection and the digital economy, and lay the groundwork for suitable and sustainable future regulation.

This document is based on the STOA study 'Blockchain and the General Data Protection Regulation - Can distributed ledgers be squared with European data protection law?' (PE 634.445). The study was written by Dr Michèle Finck at the request of the Panel for the Future of Science and Technology (STOA) and managed by the Scientific Foresight Unit, within the Directorate-General for Parliamentary Research Services (EPRS) of the European Parliament. STOA administrator responsible: Mihalis Kritikos.

stoa@ep.europa.eu (contact)

http://www.europarl.europa.eu/stoa/ (STOA website)

www.europarl.europa.eu/thinktank (internet)

http://epthinktank.eu (blog)