MIT Computational Law Report

Unblocking blockchain data flows in the wake of □□□□□□□ □□

Elizabeth Renieris, Dazza Greenwood

Published on: Aug 14, 2020

License: Creative Commons Attribution 4.0 International License (CC-BY 4.0)

> ***Disclaimer**: this article is not intended to constitute legal advice; instead, all information, content, and materials available on this site are for general informational purposes only.*

Introduction

In this post, we explore how the widely used model of "System Rules" for multi-party transactional and operations networks could provide a basis in fact and in law for blockchain networks to operate as a new type of conglomerated legal entity. This entity could thereby take advantage of "Binding Corporate Rules" as a way to ensure adequate protection of personal data in the aftermath of *Schrems II*, wherein the European Court of Justice invalidated the EU/US Privacy Shield arrangement. The overarching rules structure applied to dynamic, decentralized networks not only creates opportunities for compliance with privacy regulations but may also provide a new, more adaptive and scalable method of doing business, forming markets, and catalyzing idea flow and innovation.

Binding Corporate Rules and Model Clauses

In order to comply with European data protection law, transfers of personal data from inside the European Economic Area (EEA), which includes the Member States of the European Union plus Iceland, Liechtenstein, Norway, and Switzerland, to a country outside the EEA (a "third country") must be pursuant to a lawful mechanism.[1]

There are three primary data transfer mechanisms for so-called "third country" or "extra-EU" transfers under current European data protection law, i.e. the General Data Protection Regulation (GDPR): (1) adequacy decisions; (2) standard contractual clauses (SCCs) (also known as "model clauses"); and (3) binding corporate rules (BCRs). The arrangement invalidated by *Schrems II* was the result of an adequacy decision by the Commission, Decision 2016/1250, about the protection for personal data provided by the EU-U.S. Privacy Shield arrangement.[2] In the wake of *Schrems II*, SCCs and BCRs are still valid, though they also face significant challenges.

Article 45 of the GDPR provides for transfers on the basis of an "adequacy decision." An adequacy decision is the means by which the European Commission determines that a third country meets the standards of data protection laid out in the GDPR and thus can adequately protect any personal data transferred to it. At present, there are only a dozen jurisdictions that have been deemed adequate by the Commission, which makes this mechanism of limited utility for large multinational corporations doing business across many countries. Adequacy decisions are subject to periodic review, and can be amended, repealed, or suspended by the Commission.

Article 46 of the GDPR allows for transfers pursuant to appropriate safeguards, including standard contractual clauses (SCCs). SCCs are standardized model contract clauses that data controllers can

incorporate into their commercial contracts when transferring personal data to entities outside of the EEA, even in the absence of an adequacy decision. The European Commission has adopted such SCCs for transferring personal data to data controllers and, more recently, to data processors such as subcontractors. While the contractual clauses themselves are standardized and non-negotiable, implementing them can still be onerous as each commercial contract has to be separately negotiated, requires determinations as to the relative roles of the parties, and considerations around the further processing (or "onward transfers") of personal data, among other requirements.

Finally, Article 47 of the GDPR allows for transfers pursuant to binding corporate rules (BCRs). BCRs are binding rules for *intra*-company or internal transfers of data within a single multinational company or organization. BCRs must contain three primary elements: (1) a commitment to the GDPR's core data protection principles (lawfulness, fairness and transparency; purpose limitation; data minimization; accuracy; storage limitation; integrity and confidentiality; and accountability of the data controller or controllers);[3] (2) tools for effectiveness, including training, audit, and enforcement mechanisms; and (3) proof of bindingness both internally (i.e. between internal entities and employees within the organization) and externally (i.e. for the benefit of individuals outside of the organization whose personal data is processed by the organization). With BCRs in place, it is much easier to allocate liability across parties and across jurisdictions.

The BCRs must be approved by a designated lead data protection authority (DPA) who then spearheads a cooperation procedure with other DPAs in the countries where the multinational is located or has operations.

Extrapolating to Blockchain

A lot of the excitement over blockchain has been generated by public permissionless blockchains (such as Bitcoin and Ethereum), which arguably offer the greatest innovation over existing data storage technologies, including traditional databases. At the same time, public permissionless blockchains of this kind face significant challenges in complying with existing laws and regulations, including the European data protection rules set out in the GDPR.

There is significant uncertainty regarding the extent to which a public permissionless ledger can adhere to some of the core data protection principles set out in Article 5 of the GDPR, particularly purpose limitation and storage limitation, due to the automatic replication of the ledger across all nodes and its permanence (techniques like "pruning" aside). Additional challenges in respect of public permissionless blockchains and the GDPR are how to give effect to certain data subject rights, especially the rights of rectification, erasure, and restriction of processing.

To the extent that such blockchains are immutable, "append-only" records, rectification can only be achieved by adding a new transaction to the ledger but not actually by rectifying or correcting an older or existing entry. Erasure is also a challenge in light of immutability, as a prior transaction may be rendered "unfound" or impossible to access by a mechanism such as a tombstone (though this is harder to achieve in a fully permissionless setting). Restriction of processing may be even harder to implement since it lacks the finality of erasure and is reversible if and when the restriction is lifted.

In addition to these challenges in respect of adhering to core principles and giving effect to data subject rights, public permissionless blockchains also face the complex challenge of achieving lawful and compliant international or cross-border data transfers, the subject of this note.

In a public permissionless blockchain, anyone can stand up a node and participate in the consensus protocol to validate transactions and maintain a copy of the ledger; in other words, they are accessible anywhere. The ledger is automatically replicated across all nodes in the network, regardless of where they are located geographically. Thus, we can presume that any public permissionless network that is accessible in the EU (i.e. any public permissionless network) will automatically transfer data outside of the EU as the ledger is replicated across all nodes of the network, wherever those nodes may be located. This means that unless such a network has a lawful mechanism in place for these extra-EU transfers, it is unlikely to comply with the requirements set out in the GDPR.

How might the model of BCRs apply to a public permissionless blockchain? Could we craft something like Binding Network Rules (BNRs) that are analogous to traditional BCRs to achieve compliant cross-border transfers on the network? Article 29 Working Party guidance ("WP guidance") has indicated that BCRs are relevant to transfers between parties "engaged in a joint economic activity." Since blockchains are used to transfer value, the nodes in the given network are arguably engaging in a joint economic activity and might be a good candidate.

So how might this work? Let's go back to three core requirements for BCRs: (1) core principles, (2) tools for effectiveness, and (3) proof of bindingness. Is there a way to program a ledger via smart contracts or code to achieve these ends? Of course, any technical implementation would need to be backed up by binding legal agreements (as the technical or code layer alone would be insufficient).

Extrapolating from standard multilateral network rules

System Rules are one possible model for applying Binding Corporate Rules to the rather novel context of open, permissionless blockchains. System Rules are a shorthand for describing a common way multiparty networks structure and enforceably agree on how the network will be organized and operated. In other words, System Rules are a legally enforceable set of specifications, rules, and agreements that governs a network made up of any number of parties.

For example, a supply chain may have an umbrella set of rules called a Trading Partner Agreement and a credit card transactional network will have an overarching set of operating rules, such as the Visa Operating Rules or Mastercard Rules. Parties operating in or through such networks enforceably agree to the overarching umbrella rules through a much shorter participation contract, such as the Merchant Agreement or the Cardholder Agreement in a credit card system. This general design pattern is widely applied in many parts of the economy and for many large scale types of networks.

One interesting domain in which System Rules are widely used are so-called "identity federations" that allow members of any participating group to login to applications or services from across the network using their own account, rather than needing login credentials for each resource. In this context System Rules are frequently called "Trust Frameworks" such as the rules governing the IDFederation used by the insurance industry in the United States. The basic design is the same across domains, featuring an umbrella set of rules governing the overall system, participation agreements signed by all parties operating or interacting through the system, and covering key business, legal and technical terms necessary to specify acceptable actions, responsibilities of all parties, ongoing decision making, technology performance and interoperability, liability, dispute resolution and other key items needed for the system to function in reliable and predictable ways.

In essence, System Rules govern and define the roles and relationships of parties, their rights and responsibilities and cover key business and operations, legal and compliance, and the technology and standards used such that the system is functional, trustworthy and yields predictable legal results.

Relevant requirements for Binding Corporate Rules

A closer look at the requirements for Binding Corporate Rules is needed to explore whether or how they might be applied in novel ways. One core requirement of BCRs is that the rules are in fact legally binding. According to the EU guidance on BCRs, they can apply to "any group of companies which are effectively bound by the rules." BCRs are primarily aimed toward "intra-corporate" contexts as a way to ensure all sub-entities of a given business comply with the rules. However, BCRs can also apply to groups of different businesses engaged in some common endeavor. When the rules are applied to multiple different legal entities, there must be an enforceable legal instrument such as a contract to ensure rules are legally binding.

What does the EU mean by the word "corporate" in the context of "Binding Corporate Rules"? The word corporate in this context extends well beyond a single company and instead can refer to a "any group of companies" operating under a single set of enforceable rules ensuring data protection. Specifically, WP guidance[4] defines the word "corporate" in the sense:

> *...that they consist of the rules in place in multinational companies, usually set up under the responsibility of the headquarters. For the purposes of this document, a corporate group* ***is any group***

> ***of companies*** *which are effectively bound by the rules…* (emphasis added)

BCRs require a "list of entities bound by BCRs" and good evidence that the rules are truly binding on all entities included. The need to specifically identify and bind all participating entities in the network in this way marks a difference with the approach of some public, open blockchains designed to obscure or make secret the participants playing various roles on the blockchain. However, having a specific point of contact acting as a headquarters and an identified set of participants that have enforceably agreed to umbrella rules is consistent with many contexts where participating businesses wish to make known (and not keep secret) their identities and prefer to operate under clear rules with predictable legal outcomes.

A blockchain or other distributed network that is organized too loosely may not be an eligible candidate for use of BCRs. Like BCRs, Standard Contractual Clauses can be used as a legal basis for data transfers between EU and non-EU countries. Incorporating the same types of overarching rules but augmented with Standard Contract Clauses could be another path forward. This novel adaptation of System Rules could help further a theory of "Binding Network Rules."

A key question is how loosely can a group of companies be while still being eligible for use of BCRs? According to Article 29 Working Party guidance,[5] there may be low tolerance for approving too loose of a conglomerate of entities.

> *For loose conglomerates, binding corporate rules are very unlikely to be a suitable tool. The diversity between their members and the broad scope of the processing activities involved would make it very difficult (if not impossible) to meet the requirements outlined in this working document. For these conglomerates it would be necessary to differentiate subgroups within the same corporate group, set up severe limitations and conditions for the exchanges of information and particularise the rules. In other words, should a final product end up being acceptable under Article 26 (2) of the Directive, it would certainly look like (sic) very different from the binding corporate rules discussed in this working document.*

According to additional WP guidance,[6] the group of companies seeking to operate under BCRs will have to explain in their application form how the rules are made binding "*between the companies/entities in the group by intra-group agreement, unilateral undertakings, internal regulatory measures, policies of the group, or other means.*" An open, permissionless blockchain could be designed to require each participating organization to identity itself and agree to such rules as part of an onboarding process. One can imagine relatively lightweight and largely automated processes that nonetheless result in valid, reliable and enforceable agreements and policies of this type, in effect legally binding each participating node in a blockchain to the requisite rules.

Likewise, the rules must also be binding on employees of each organization "*by one or more of the following: individual and separate agreement/undertaking with sanctions, clause in employment contract with sanctions, internal policies with sanctions, or collective agreements with sanctions.*" Again, such agreements can be formed, executed, documented and verified using common tools such as DocAssemble and confirmed by each participating organization to the node responsible to conveying compliance to the relevant EU regulatory body.

The formal application for Binding Corporate Rules requests: "*What verification mechanisms does your Group have in place to audit each member's compliance with your BCRs? (e.g., an audit programme, compliance programme, etc)?*" There are many ways to verify audit of compliance with data protection rules, and the presence of such a program is another example of a best practice that would not only enable cross-border data transfer but also promote the general integrity and trustworthiness of distributed networks.

These requirements for seeking approval of BCRs can all be satisfied implicitly by use of the clauses commonly included in "System Rules" approaches to organizing multiparty participation across a network. What's more, these items are at once incredibly useful for structuring the transactions, governance and operation of any confederation or other association of separate organizations working in concert together. The approach to seeking approval of BCR's for open, public blockchains through the general design pattern of System Rules could provide important missing business and legal certainty that has thus far been inhibiting widespread adoption of this blockchain technology.

Conclusion

Therefore, if System Rules are designed for and executed by groups of entities operating on blockchain or other distributed networks in a way that addresses the requirements of Binding Corporate Rules, then participants can resolve the uncertainty resulting from *Schrems II* by establishing a kind of Binding Network Rules. Such Binding Network Rules could also provide the basis for addressing much of the current legal and business uncertainty associated with relying on blockchains as the means for conducting important transactions beyond the transfer of cryptocurrency.

While the process of designing, obtaining approval, and maintaining Binding Corporate Rules is challenging, it may be a promising solution to ecosystems that can establish a corporate group in a post-*Schrems II* environment. By extension, that could unlock the potential of Binding Network Rules for blockchain networks.

Elizabeth Renieris (CIPP/E, CIPP/US) is a privacy lawyer, the founder & CEO of HACKYLAWYER, and a fellow at the Berkman Klein Center for Internet & Society and the Carr Center for Human Rights Policy at

Harvard University. Elizabeth is on the Board of Advisors for the MIT Computational Law Report.

Daniel "Dazza" Greenwood is a researcher at MIT Media Lab and Lecturer at Connection Science, in the MIT School of Engineering, where he is advancing the field of computational law and building out Law.MIT.edu research portfolio. Dazza is also founder of CIVICS.com, a boutique provider of professional consultancy services for legal technologies, automated transactions, data management and technology strategy.

Footnotes

1. *See* Article 44, GDPR. ↩

2. Although not the focus here, there also continue to be a number of derogations permitting transfers of personal data in limited circumstances, which are similar to existing derogations, and include: explicit consent, contractual necessity, important reasons of public interest, legal claims, vital interests, and public register data. *See* Article 49, GDPR. ↩

3. *See* Chapter II, GDPR. ↩

4.
See Working Document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers" (3 June 2003).

↩

5. Working Document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, adopted 3 June 2003. ↩

6. Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, document 1271-00-00/08/EN WP 153 as adopted on 24 June 2008. ↩