17 April 2023

An Open Letter to Representatives of the European Parliament, the Council of the European Union, and the European Commission

In re: Amendments to Article 30 of the Data Act To Clarify Its Limited Scope

Polygon Labs, an international software development company that builds blockchain infrastructure solutions, writes to address concerns relating to Article 30 ("Art. 30") of the Data Act. Specifically, we seek to clarify the scope and intent of Art. 30 to ensure it accounts for the ways in which smart contracts operate and the potential negative consequences of imposing a requirement for "safe termination or interruption" of such smart contracts in *permissionless* systems. We propose amendments to narrow the scope of Art. 30 to ensure it applies, at most, to *permissioned* smart contract based-systems owned and operated by an identifiable natural person or corporate entity (*i.e.*, an "enterprise" under the Data Act's definitions) who has entered into a traditional contractual agreement for the sharing of "personal data" as defined by the Data Act.

Polygon Labs has an interest in this matter because we seek to ensure the growth and responsible development of permissionless blockchain-based systems globally. Third-party developers have built and deployed robust smart contract-based applications onto various permissionless blockchain networks developed by Polygon Labs. We seek to ensure that software developers, both in the European Union ("EU") and abroad, can continue to innovate with smart contracts. For these reasons and those discussed below, Ledger, a French company and leading provider of security solutions for digital assets, joins in this letter.

Accordingly, we offer suggested revisions to certain language of Art. 30 to ensure the final text reflects the EU's objectives for this provision—namely, "removing barriers to the development of the European data economy in compliance with European rules and fully respecting European values, and in line with the mission to reduce the digital divide so that everyone benefits from these opportunities".[1] We respectfully request that you consider the proposed revisions to Art. 30 discussed below to ensure that this new law does not inadvertently capture open, transparent and permissionless parts of emerging blockchain technology.

Specific Comments on Article 30

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022PC0068&from=EN ("Data Act Text") at ¶ 1.

For the purposes of this letter, we will refer to the following text of Art. 30, as outlined by the European Parliament,[2] and only comment on the parts of the provision that need further refinement to address the realities of the technology and achieve the EU's goals as stated in the Data Act.
For ease of reference, we provide the full text of Art. 30 below.

Article 30[3]

Essential requirements regarding smart contracts for data sharing

*▌The **party offering** smart contracts ▌in the context of an agreement to make data available shall comply with the following essential requirements:*

*(a) robustness **and access control**: ensure that the smart contract has been designed to offer rigorous access control mechanisms and a very high degree of robustness to avoid functional errors and to withstand manipulation by third parties;*

*(b) safe termination and interruption: ensure that a mechanism exists to terminate the continued execution of transactions: the smart contract shall include internal functions which can reset or instruct the contract to stop or interrupt the operation to avoid future (accidental) executions; **in this regard, the conditions under which a smart contract could be reset or instructed to stop or interrupted, should be clearly and transparently defined. Especially, it should be assessed under which conditions non-consensual termination or interruption should be permissible;***

(ba) equivalence: a smart contract shall afford the same level of protection and legal certainty as any other contracts generated through different means.

(bb) protection of confidentiality of trade secrets: ensure that a smart contract has been designed to ensure the confidentiality of trade secrets, in accordance with this Regulation.

Our concerns with Art. 30 pertain to certain language that broadens its scope so widely that it could have the unintended effect of prohibiting permissionless, autonomous smart contracts and the applications based thereon – specifically, the clause in the preamble to Art. 30 – "[t]he party offering smart contracts in the context of an agreement to make data available".

Without a more precise definition of both (1) "the party offering" (to exclude software developers), and (2) "an agreement to make data available" (to apply only to "enterprises" and "personal data" as those terms are defined in the Data Act), Art. 30's preamble will inadvertently capture a significant

[2] Data Act Text at Art. 30 (pp. 57-58) (emphasis in original). This version of the text clarifies some of the ambiguity in the European Commission's proposal (*e.g.*, "vendor of an application using smart contracts").

[3] https://www.europarl.europa.eu/doceo/document/A-9-2023-0031_EN.html#_section1 (emphasis in original).

number of smart contracts, many of which have ***no*** "party offering" them and, as such, will not have the ability to comply with the requirements in Art. 30, including and especially the requirement that such smart contract systems have the ability to be "terminated or interrupted". This is especially so because many smart contracts "make data available"; in fact, that is the explicit purpose of many smart contracts and, arguably, all smart contracts.

Critically, Art. 30 as drafted would not be enforceable for open, permissionless and decentralized smart contract applications and would substantially inhibit innovation and economic growth in the EU, in direct contravention of the intention behind the EU's Markets in Cryptoassets regulation ("MiCA").[4] Thus, we propose amendments to certain parts of Art. 30 to ensure that the provision remains in line with the goal of the Data Act—to ensure the protection of all uses of data.

"The party offering smart contracts in the context of an agreement to make data available shall comply with the following essential requirements . . ."

Clarify the term "party offering smart contracts" to exclude software developers of decentralized protocols and applications.

Smart contracts are the backbone of many applications built upon permissionless, blockchain-based software. Truly decentralized applications (or "dApps") – built through smart contracts – do not have ***any*** "party offering" them; rather, software developers write the smart contract code and then publish it (also called "deploying") to a permissionless blockchain network such as Ethereum. Once deployed, those dApps can run on the permissionless blockchain network without any intervention. Through wallets or directly on a permissionless blockchain network, users guide and control their interactions and transactions with dApps.

Given the autonomous nature of dApps and that no party "offers" them, we propose the EU include a specific amendment to Art. 30 to exclude software developers – those who write and publish code – from the scope of the provision to ensure that those engaged in software development are not inadvertently considered a "party offering" smart contracts. Any ambiguity around this point will unnecessarily chill innovation in the EU and run contrary to MiCA's exclusion of "crypto-asset services . . . provided in a fully decentralized manner".[5]

We recognize that some applications – even if using the nomenclature "decentralized" or "dApp" – may have points of centralization or may have a "party" (*i.e.*, an identifiable natural person or traditional corporate entity) controlling the software such that they fall under Art. 30. With the narrow "software developer" exclusion suggested above, Art. 30 would still capture these natural persons or corporate entities providing centralized – or even partially centralized – services through smart contracts. Failing to include a "software developer" exclusion would continue to (unintentionally) render Art. 30 overly broad.

[4] https://www.europarl.europa.eu/doceo/document/A-9-2022-0052-AM-002-002_EN.pdf.
[5] *See* https://data.consilium.europa.eu/doc/document/ST-13198-2022-INIT/en/pdf.

Clarify that "an agreement to make data available" applies only to traditional contractual agreements between or among two natural persons or traditional corporate entities for the purposes of sharing confidential personal and business data.

The Data Act's sweeping definition of "data" expands the scope of Art. 30 to capture nearly any type of smart contract. Here, "data" means "any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audio-visual recording; content, or data obtained, generated or collected by the connected product or transmitted to it on behalf of others for the purpose of storage or processing, shall not be covered by this Regulation."[6]

This definition of "data" encapsulates any type of information that may be shared between and among persons via smart contracts. Smart contracts, by their nature, share data or otherwise make data available – to each other and to the users of the smart-contract based applications, whether decentralized or otherwise. They share "acts, facts or information" or "any compilation" thereof in dApps or permissioned systems. Accordingly, Art. 30 would capture every smart contract based system. We do not believe, based on the Data Act's stated purpose, that is the intention of this regulation.

The requirements for smart contracts in provisions (a) through (bb) of Art. 30 make clear that the provision is intended to protect particularly sensitive "data" or information, as does the preamble to the Data Act—specifically, "personal data"[7] and "confidential business data and trade secrets".[8] This intention can be used to provide appropriate scope for Art. 30.

Based on the above, we propose two additional amendments:

(1) Add a clause that makes clear the term "an agreement to make data available" applies to contractual agreements between two "enterprises" (as defined by the Data Act)[9] and does not apply to smart contract-based agreements themselves;` and
(2) Provide language to narrow the scope of the purpose of any "agreement" at issue under Art. 30 to "personal data"[10] and "confidential business data and trade secrets".

---

[6] Data Act Text, Art. 2(1).
[7] *See* Data Act Text, Whereas, Clause 7 (addressing the "fundamental right to the protection of personal data").
[8] *See, e.g.*, Data Act Text at p.2.
[9] Data Act Text, Art. 2(8).
[10] "Personal data" under the Data Act has the same meaning as in Article 4, point (1), of Regulation (EU) 2016/679, Data Act, Art. 2(1a), which defines "personal data" as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".

Accordingly, the provision would read: "~~*The party*~~ ***An enterprise*** *offering smart contracts in the context of an agreement* ***with another enterprise*** *to make* ***personal*** *data* ***or confidential business data and trade secrets*** *available*".

"(b) safe termination and interruption; ensure that a mechanism exists to terminate the continued execution of transactions: the smart contract shall include internal functions which can reset or instruct the contract to stop or interrupt the operation to avoid future (accidental) executions; in this regard, the conditions under which a smart contract could be rest or instructed to stop or interrupted, should be clearly and transparently defined. Especially, it should be assessed under which conditions non-consensual termination or interruption should be permissible"

Clarify that this would exclusively apply to *permissioned* smart contracts which are owned and operated by an "enterprise".

Smart contracts deployed to permissionless blockchain networks operate autonomously – *i.e.*, without human intervention. When those applications are "fully decentralized" (as that term has been used in MiCA), no one controls them.

By imposing a function that allows a protocol to be "terminat[ed] or interrupt[ed]", Art. 30(b) appears to force the existence of a centralized party in a smart contract-based system who can shut down or otherwise amend or interrupt the smart contracts. Without the amendments proposed above and below, this "centralizing" requirement in Art. 30 will inadvertently eliminate the existence of permissionless smart contract-based systems.

This effect of Art. 30 will stand in stark contrast to the current policies for blockchain-based software set forth by the EU, including MiCA, which excludes "crypto-asset services . . . provided in a fully decentralized manner" from the scope of the regulation at this time.[11] Art. 30 should remain consistent with MiCA in keeping decentralized, autonomous systems out of regulatory scope.

To avoid this unintended consequence of Art. 30, two further amendments should be made to Art. 30:

(1) State that Art. 30 applies only to *permissioned* systems owned and/or operated by an "enterprise" as defined by the Data Act; and

(2) Import language similar to the language of MiCA to exclude "crypto-asset services . . . provided in a fully decentralized manner" from the scope of Art. 30.

"Provisions (a), (ba), (bb)."

[11] *See* https://data.consilium.europa.eu/doc/document/ST-13198-2022-INIT/en/pdf.

If the EU government implements the amendments outlined above, then provisions *(a)*, *(ba)*, and *(bb)* need no further clarity. Without these revisions, additional amendments will be necessary to sections (a), (ba) and (bb) of Art. 30 to limit their scope to permissioned systems operated by an "enterprise".

* * *

We understand that policymakers did not intend to regulate software so widely as the text of Art. 30 currently suggests. Therefore, we have provided the needed clarifications for Art. 30, in its current form, to meet the goals set out by the EU in the Data Act as well as protect novel, permissionless technology. As mentioned previously, the scope of Art. 30 should only capture permissioned smart contract-based systems owned and operated by an "enterprise" who has entered into a contractual agreement for the sharing of "personal data" or "confidential business data or trade secrets".

To ensure that Art. 30 promotes continued innovation, remains aligned with the EU's other regulations relating to blockchain-based software, and allows for compliance by any parties falling within the scope of Art. 30, we respectfully request that the above amendments be implemented prior to enactment of the Data Act.

We recognize and appreciate the EU's efforts to explore new technology, especially in ways that could benefit the EU economy, and welcome the opportunity to provide additional information or proposed amendments as you continue to refine this legislation.

We are available for further discussion at policy@polygon.technology and appreciate your consideration on this important matter.