A Data-Driven Analysis of Blockchain Systems' Public Online Communications on GDPR: Supplementary Material

Rahime Belen Sağlam, Çağrı B. Aslan, Shujun Li, Lisa Dickson and Ganna Pogrebna

July 27, 2020

1 Introduction

This is supplementary material for the following paper:

Rahime Belen Sağlam, Çağrı B. Aslan, Shujun Li, Lisa Dickson and Ganna Pogrebna, "A Data-Driven Analysis of Blockchain Systems' Public Online Communications on GDPR," in *Proceedings of 2020 IEEE International Conference on Decentralized Applications and Infrastructures* (IEEE DAPPS 2020), pp. 22-31, 2020, IEEE, DOI:10.1109/DAPPS49028.2020.00003

2 Cryptocurrencies Studied

The 320 cryptocurrencies studied in the above-mentioned paper are (as listed on CoinMarketCap, ranked according to the market capital size as of 17 April 2019 08:42:19 UK time; cryptocurrencies belonging to the same company are grouped together using the word "and" and those cryptocurrencies are ranked based on their collective market capital size): Bitcoin, Ethereum, XRP, Bitcoin Cash, EOS, Litecoin, Binance Coin, Tether, Stellar, Cardano, TRON, Monero, Dash, Bitcoin SV, IOTA, Tezos, NEO and Gas, Ethereum Classic, Ontology, Maker and Dai, NEM, Zcash, Crypto.com Chain (CRO) and Crypto.com (MCO, formerly known as Monaco), Basic Attention Token, VeChain, Dogecoin, Bitcoin Gold, OmiseGO, Waves, USD Coin, Qtum, Lisk, Decred, Augur, Nano, TrueUSD, Ravencoin, 0x, Zilliqa, Holo, Chainlink, ICON, BitShares, Bytecoin, Bitcoin Diamond, BitTorrent, IOST, DigiByte, Aeternity, Maximine Coin, Verge, Pundi X, Steem, Siacoin, Enjin Coin, Bytom, Komodo, THETA, Huobi Token, Paxos Standard Token, KuCoin Shares, Aurora, Stratis, Status, ABBC Coin, Waltonchain, Mixin, Insight Chain, Digitex Futures, Golem, Factom, Project Pai, WAX, Ardor and Ignis, GXChain, Cryptonex, Populous, Qubitica, Ark, ThoreCoin, VestChain, MaidSafeCoin, Gemini Dollar, HyperCash, Nebulas, NULS, Revain, Loopring, Zcoin, Decentraland, Elastos, Aion, TrueChain, PIVX, Loom Network, WaykiChain, REPO, aelf, Bibox Token, Lambda, Electroneum, QuarkChain, QASH, ReddCoin, Power Ledger, Horizen, Wanchain, Kyber Network, Nexo, MOAC, Bancor, Dent, Metaverse ETP, MonaCoin, LATOKEN, IoTeX, Santiment Network Token, Storj, RIF Token, iExec RLC, Polymath, DigixDAO, Kin, Celer Network, Enigma, ODEM, TomoChain, STASIS EURS, FunFair, Nxt, Obyte, Linkey, Groestlcoin, Veritaseum, Davinci Coin, TenX, Syscoin, Centrality, CyberMiles, Cindicator, MediBloc [ERC20] (MEDX) and MediBloc [QRC20] (MED), Metadium, Apollo Currency, Buggyra Coin Zero, Bread, Dragonchain, Cred, Clams, Cortex, Civic, Odyssey, Mainframe, Arcblock, Quant, ProximaX, Vertcoin, Ecoreal Estate, #MetaHash, Metal, TokenClub, TokenPay, SingularityNET, Matrix AI Network, Neblio, Mithril, Moeda Loyalty Points, Nexus, Tael, Grin, S4FE, Energi, Ankr Network, Particl, TTC Protocol, Spectre.ai Dividend Token, CRYPTO20, Cosmo Coin, Skycoin, Telcoin, INO COIN, TokenCard, United Traders Token, Einsteinium, BnkToTheFuture, High Performance Blockchain, WhiteCoin, BitKan, GoChain, SmartCash, Request, Fusion, Aragon, Endor Protocol, Storm, Gifto, Eidoo, Wagerr, Smartlands, Po.et, Everex, Gnosis, Asch, Cube, Nectar, BitCapitalVendor, Robotina, Everipedia, Dynamic Trading Rights, SmartMesh, Ren, Quantstamp, Unobtanium, Genesis Vision, HYCON, SIRIN LABS Token, CWV Chain, Streamr DATAcoin, PTON, OST, STEM CELL COIN, Raiden Network Token, UTRUST, Ripio Credit Network, OneRoot Network, Iconomi, Fetch, Ethos, CyberVein, OriginTrail, Namecoin, Blocknet, NKN, PLATINCOIN, Peercoin, NavCoin, THEKEY, Bezant, Clipper Coin, Hyperion, Bluzelle, Gold Bits Coin, Dentacoin, IHT Real Estate Protocol, Time New Bank, FLO, PressOne, Emercoin, MediShares, Humanscape, Moss Coin, SCRL, Crypterium, Ruff, Bitcoiin, Dropil, Credits, Fantom, CasinoCoin, Own, Viacoin, Noah Coin, Achain, APIS, Numeraire, DEX, LockTrip, BHPCoin, Substratum, Propy, eosDAC, RChain, Scry.info, DeepBrain Chain, SALT, AdEx, ETHLend, Edgeless, Quantum Resistant Ledger, DATA, PumaPay, DMarket, SOLVE, DEW, Nucleus Vision, FirstBlood, BitNewChain, Game.com, Aergo, VIBE, DigitalNote, VITE, IoT Chain, bitCNY, BLOCKv, SDChain, ZelCash, Insolar, BridgeCoin, Credo, EDUCare, Red Pulse Phoenix, SONM, XYO, ZClassic, Tokenomy, district0x, All Sports, XcelToken, NEXT, SingularDTV, Ubiq, Spectrecoin, BitBay, Beam, Tripio.

3 Selected "Good" Privacy Policies Mentioning GDPR

In our data-driven analysis of public online communications of blockchain systems' developers and service providers, we noticed a number of good examples of privacy policies that discuss GDPR key principles in a more transparent manner. In this section we give some examples, quoting important texts appearing in relevant legal documents directly, including the original text styles (color and any other highlighting).

3.1 Examples from the 314 investigated blockchain systems

3.1.1 GNOSIS

GNOSIS's privacy policy[1] is among the most transparent ones in terms of communicating potential loss of data subjects' rights defined in the GDPR. It has very detailed discussions on all important aspects of GDPR and repeatedly reminded its users about the potential loss of some data subjects' rights.

In "2. Your information and the Blockchain" it says

> "Accordingly, by design, a blockchains records cannot be changed or deleted and is said to be 'immutable'. This may affect your ability to exercise your rights such as your right to erasure ('right to be forgotten'), or your rights to object or restrict processing, of your personal data. Data on the blockchain cannot be erased and cannot be changed. Although smart contracts may be used to revoke certain access rights, and some content may be made invisible to others, it is not deleted.
>
> ...
>
> IF YOU WANT TO ENSURE YOUR PRIVACY RIGHTS ARE NOT AFFECTED IN ANY WAY, YOU SHOULD NOT TRANSACT ON BLOCKCHAINS AS CERTAIN RIGHTS MAY NOT BE FULLY AVAILABLE OR EXERCISABLE BY YOU OR US DUE TO THE TECHNOLOGICAL INFRASTRUCTURE OF THE BLOCKCHAIN.IN PARTICULAR THE BLOCKCHAIN IS AVAILABLE TO THE PUBLIC AND ANY PERSONAL DATA SHARED ON THE BLOCKCHAIN WILL BECOME PUBLICLY AVAILABLE"

In "3.4 When participating in the OWL generation" and "3.7 Deploying a MultiSig and making transactions" it further says

> "THE DATA WILL BE STORED ON THE ETHEREUM BLOCKCHAIN. GIVEN THE TECHNOLOGICAL DESIGN OF THE BLOCKCHAIN, AS EXPLAINED IN SECTION 2, THIS DATA WILL BECOME PUBLIC AND IT WILL NOT LIKELY BE POSSIBLE TO DELETE OR CHANGE THE DATA AT ANY GIVEN TIME."

In "4.6 Ethereum Blockchain" the policy says

> "THE INFORMATION WILL BE DISPLAYED PERMANENTLY AND PUBLIC, THIS IS PART OF THE NATURE OF THE BLOCKCHAIN. IF YOU A NEW TO THIS FIELD, WE HIGHLY RECOMMEND INFORMING YOURSELF ABOUT THE BLOCKCHAIN TECHNOLOGY BEFORE USING OUR SERVICES."

In "6. Transferring Your data outside of the EU" it says

> "HOWEVER, WHEN INTERACTING WITH THE BLOCKCHAIN, AS EXPLAINED ABOVE IN THIS POLICY, THE BLOCKCHAIN IS A GLOBAL DECENTRALIZED PUBLIC NETWORK AND ACCORDINGLY ANY PERSONAL DATA WRITTEN ONTO THE BLOCKCHAIN MAY BE TRANSFERRED AND STORED ACROSS THE GLOBE"

In "9. Your Rights as a Data Subject" and under "Right to erasure (right to be 'forgotten')", the policy says

> "HOWEVER, WHEN INTERACTING WITH THE BLOCKCHAIN WE MAY NOT BE ABLE TO ENSURE THAT YOUR PERSONAL DATA IS DELETED. THIS IS BECAUSE THE BLOCKCHAIN IS A PUBLIC DECENTRALIZED NETWORK AND BLOCKCHAIN TECHNOLOGY DOES NOT GENERALLY ALLOW FOR DATA TO BE DELETED AND YOUR RIGHT TO ERASURE MAY NOT BE ABLE TO BE FULLY ENFORCED. IN THESE CIRCUMSTANCES WE WILL ONLY BE ABLE TO ENSURE THAT ALL PERSONAL DATA THAT IS HELD BY US IS PERMANENTLY DELETED."

Under "Right to restrict processing and right to object to processing" it says

[1] `https://gnosis.io/privacy-policy`

"HOWEVER, WHEN INTERACTING WITH THE BLOCKCHAIN, AS IT IS A PUBLIC DECENTRALIZED NETWORK, WE WILL LIKELY NOT BE ABLE TO PREVENT EXTERNAL PARTIES FROM PROCESSING ANY PERSONAL DATA WHICH HAS BEEN WRITTEN ONTO THE BLOCKCHAIN. IN THESE CIRCUMSTANCES WE WILL USE OUR REASONABLE ENDEAVOURS TO ENSURE THAT ALL PROCESSING OF PERSONAL DATA HELD BY US IS RESTRICTED, NOTWITHSTANDING THIS, YOUR RIGHT TO RESTRICT TO PROCESSING MAY NOT BE ABLE TO BE FULLY ENFORCED."

3.1.2 Holo

Holo's privacy policy has a section "3.3. Ethereum Blockchain" that states the following:

> "by design, a blockchain's records cannot be changed or deleted and is said to be 'immutable'. This may affect your ability to exercise your rights such as your right to erasure ('right to be forgotten'), or your rights to object or restrict processing, of your Personal Data.
>
> **Given the technological design of the blockchain, certain data stored on it (which may include Personal Data) will become public and it will not likely be possible to delete or change the data at any given time. If you want to ensure your privacy rights are not affected in any way, you should not transact on blockchains.**"

3.1.3 MediBloc

MediBloc's privacy policy[2] also warned its users with the statements in "Article 28 (Your Information and the Blockchain)":

> "Accordingly, by design, a blockchain's records cannot be changed or deleted and is said to be immutable. This may affect your ability to exercise your rights such as your right to erasure ('right to be forgotten'), the right to rectification of your data or your rights to object or restrict processing, of your personal data. Data on the blockchain cannot generally be erased or changed, although some smart contracts may be able to revoke certain access rights, and some content may be made invisible to others, however it is not deleted.
>
> ...
>
> IF YOU WANT TO ENSURE YOUR PRIVACY RIGHTS ARE NOT AFFECTED IN ANY WAY, YOU SHOULD NOT TRANSACT ON BLOCKCHAINS OR USE THE SERVICES PROVIDED BY MediBloc AS CERTAIN RIGHTS MAY NOT BE FULLY AVAILABLE OR EXERCISABLE BY YOU OR BY MediBloc.
>
> IN PARTICULAR, THE BLOCKCHAIN IS AVAILABLE TO THE PUBLIC AND ANY PERSONAL DATA SHARED ON THE BLOCKCHAIN WILL BECOME PUBLICLY AVAILABLE."

3.1.4 OST

OST's privacy policy[3] has two separate sections for the personal data processed during the use of their platform and the the website services. The users were informed about the personal data stored in the blockchain as follows:

> "OST Platform is a blockchain-technology based service. OST makes its best efforts to collect as little personal data from its clients and their users as possible. Regarding our clients' end users, there are only two personal data parameters that are saved on OST Platform;
>
> 1. The end user email address for redemption options
> 2. The end user's unique id
>
> The unique id is created on OST Platform to allow our clients to map their own users with the information existing on the clients' side. The user id is not publicly available and only shared between OST and the client. OST does not know the identity behind the unique id; only the client which this user belongs to can associate this unique id with the user."

The policy also explains their approach to overcoming immutability problem with the following statements:

> "Being a blockchain-technology based service, transactions executed on the blockchain are public and cannot be deleted. However, in order to comply with the user's right to be forgotten, we take measures when a user wants his/her personal data to be removed from OST Platform by deleting all blockchain identifiers associated with the user id."

[2] https://docs.medibloc.org/PrivacyPolicy_ENG.pdf
[3] https://ost.com/privacy

3.1.5 CasinaCoin

Another approach about immutability of the personal data is explained in the privacy policy of CasinaCoin[4] as follows:

> "The nature of blockchain technology means that any data entered onto a blockchain cannot be deleted; however, all such data is pseudo-anonymized which means that the data by itself on the blockchain does not reveal any personal data."

3.1.6 Solve.Care

Solve.Care[5] informed the users about personal data storage with the following statements:

> "Solve.Care uses both public and private blockchain technology. None of your personal information is stored by us in any blockchain. The only data stored in a blockchain will be your Wallet ID, Transaction Amount, and Destination Wallet ID."

3.2 Examples beyond the 314 investigated blockchain systems

Beyond the 314 block systems, we also noticed some other smaller blockchain systems whose privacy policies explicitly acknowledged the GDPR compliance issue. One such example is Bloom (associated with a cryptocurrency BLT, whose market capitalization size was $3,420,271 as of 19 April 2019 08:42:19 UK time), whose privacy policy[6] was updated on May 24, 2018, one day before the GDPR became effective. It explicitly warned its users about the GDPR compliance issue in block letters:

> "Accordingly, by design, a blockchain's records cannot be changed or deleted and is said to be 'immutable'. This may affect your ability to exercise your rights such as your right to erasure ('right to be forgotten'), the right to rectification of your data or your rights to object or restrict processing, of your personal data. Data on the blockchain cannot generally be erased or changed, although some smart contracts may be able to revoke certain access rights, and some content may be made invisible to others, however it is not deleted.
>
> ...
>
> **IF YOU WANT TO ENSURE YOUR PRIVACY RIGHTS ARE NOT AFFECTED IN ANY WAY, YOU SHOULD NOT TRANSACT ON BLOCKCHAINS OR USE THE BLOOM APP AS CERTAIN RIGHTS MAY NOT BE FULLY AVAILABLE OR EXERCISABLE BY YOU OR US.**
>
> **IN PARTICULAR THE BLOCKCHAIN IS AVAILABLE TO THE PUBLIC AND ANY PERSONAL DATA SHARED ON THE BLOCKCHAIN WILL BECOME PUBLICLY AVAILABLE.**"

It also explicitly listed information written to the blockchain:

- "the cryptographic wallet address from which you submitted the transaction;"
- "the amount of the cryptocurrency which you send as payment;"
- "the cryptographic wallet address to which you initiated the transaction;"
- "the cryptographic signature of a piece of your identity data such as phone number or date of birth; and/or"
- "the cryptographic wallet address of the entity with which you engaged in an identity attestation."

The policy also gave very detailed information about how data is processed and why it is needed. Data subjects' individual rights are also explained one by one. Interestingly, for the right to erasure, it says

> "However, when interacting with the blockchain, as explained above in this Policy, it will likely not be able to erase and permanently delete personal data which has been written onto the blockchain. In these circumstances, we will use our reasonable endeavours to ensure that all personal data held by us is permanently deleted. However, notwithstanding this, your right to erasure may not be able to be fully complied with."

For "Right to restrict processing and right to object to processing", the policy said

[4] `https://casinocoin.org/privacy-policy/`
[5] `https://solve.care/docs/solve-care-website-privacy-policy/solve-care-website-privacy-policy.pdf`
[6] `https://bloom.co/legal/privacy/`

> "However, when interacting with the blockchain, as explained above in this Policy, it will likely not be able to prevent external parties from processing any personal data which has been written onto the blockchain. In these circumstances we will use our reasonable endeavours to ensure that all processing of personal data held by us is restricted, notwithstanding this, your right to restrict to processing may not be able to be fully enforced."

When talking about "Transferring your information outside of the European Economic Area", the policy stated

> "However, when interacting with the blockchain, as explained above in this Policy, the blockchain is a global decentralized public network and accordingly any personal data written onto the blockchain may be transferred and stored across the globe."

4 Detailed Scheme for Encoding GDPR Principles

In this section we list the detailed encoding scheme we followed for analyzing legal documents of blockchain systems. For each encoding label we also give one example to further illustrate the meaning of the encoding.

4.1 Explicit Consent

Table 1: Encoding Scheme for Explicit Consent

Code	Description	Example
None	This right is not covered explicitly.	NA
Vague statements	It is not explicitly written how they obtain consent from the users.	"By providing us with your personal data, you consent to your personal data transfer, storage and processing."[7]
Via use of website or the application	Users are assumed to consent processing of their personal data when they use their Website or the application.	"You agree and understand that by visiting, accessing, or using Gemini, you are consenting to the policies and practices of our privacy policy (the 'Privacy Policy') so please read them carefully."[8]
Via use of the app	Users are assumed to consent processing of their personal data when they use the application	"Breadwinner AG ('us', 'we', or 'our') operates the brd.com website and the BRD mobile application (the 'Service') ... By using the Service, you agree to the collection and use of information in accordance with this policy."[9]
Via registration	Consent is obtained from the user as they register to their platforms, submit information to their systems or use their services	"For current members, we process your information based on the consent you have previously given us during registration."[10]
Via contract	Consent is obtained by the active submission of the wallet address or after the fulfillment of the contract between user and the system	"The legal basis for this processing is that it is necessary to fulfil a contract with you."[11]

4.2 Right to Withdraw Consent

[7] https://cryptonex.org/help/terms
[8] https://gemini.com/privacy-policy/
[9] https://brd.com/privacy
[10] https://cubeint.io/privacy-policy/
[11] https://gnosis.pm/privacy-policy

Table 2: Encoding Scheme for Right to Withdraw Consent

Code	Description	Example
None	Policy does not specifically discuss the data subject's ability to withdraw consent.	NA
Vague statements	Policy claims to support the right but without giving any further information as to how a user can withdraw her consent while using the application	"Data Subjects in the EEA or the Channel Islands may withdraw consent at any time where consent is the lawful basis for processing their Personal Information."[12]
Via email	Policy recognizes this right and require the data subject to email an express request to exercise withdrawal of consent, or to opt out a link.	"Where you have provided your consent to us processing your personal data, you can withdraw your consent at any time by clicking on this opt-out link."[13]
Immutability	Policies explicitly state that the immutability of blockchain systems may affect the users' ability to exercise this right.	"You also have the right to object to processing of your personal information under certain circumstances, such as where the processing is based on your consent and you withdraw that consent. This may impact the services we can provide and we will explain this to you if you decide to exercise this right. HOWEVER, WHEN INTERACTING WITH THE BLOCKCHAIN, AS IT IS A PUBLIC DECENTRALIZED NETWORK, WE WILL LIKELY NOT BE ABLE TO PREVENT EXTERNAL PARTIES FROM PROCESSING ANY PERSONAL DATA WHICH HAS BEEN WRITTEN ONTO THE BLOCKCHAIN. IN THESE CIRCUMSTANCES WE WILL USE OUR REASONABLE ENDEAVOURS TO ENSURE THAT ALL PROCESSING OF PERSONAL DATA HELD BY US IS RESTRICTED, NOTWITHSTANDING THIS, YOUR RIGHT TO RESTRICT TO PROCESSING MAY NOT BE ABLE TO BE FULLY ENFORCED."[14]

4.3 Right to Erasure

Table 3: Encoding Scheme for Right to Erasure

Code	Description	Example
None	This right is not covered explicitly.	NA
Erasable	Policy states that personal data can be deleted upon request and does not provide any further discussion.	"To the extent required by law, Horizen complies with the EU General Data Protection Regulation (GDPR). GDPR gives users the following rights: Right of erasure (right to be forgotten) ..."[15]
Immutable	Policy states that the application is blockchain enabled that does not allow erasure due to its nature.	"Accordingly, by design, a blockchain's records cannot be changed or deleted and is said to be 'immutable'. This may affect your ability to exercise your rights such as your right to erasure ('right to be forgotten'), the right to rectification of your data or your rights to object or restrict processing, of your personal data."[16]

continues on next page

[12] https://gemini.com/privacy-policy/
[13] https://lisk.io/privacy
[14] https://gnosis.io/privacy-policy

continued from previous page

Code	Description	Example
Anonymization	Policy states that even though data cannot be deleted due to nature of blockchain, some other techniques (anonymization or deleting all blockchain identifiers associated with the user id) will be applied to comply with the right.	"Being a blockchain-technology based service, transactions executed on the blockchain are public and cannot be deleted. However, in order to comply with the user's right to be forgotten, we take measures when a user wants his/her personal data to be removed from OST Platform, by deleting all blockchain identifiers associated with the user id."[17]
No personal data on blockchain	Policy explicitly states that personal data is not stored on the blockchain.	"None of your personal information is stored by us in any blockchain. The only data stored in a blockchain will be your Wallet ID, Transaction Amount, and Destination Wallet ID."[18]

4.4 Transparency

Table 4: Encoding Scheme for Transparency

Code	Description	Example
None	Personal data collected is not stated explicitly.	NA
Personal data limited to website services	Transparency of the policy is limited to personal data collected by website services, not the application.	"We automatically collect usage information that allows us to collect information regarding how users access and use the Services ('Usage Data'). For example, when you download and use the Services, we automatically collect information on the type of device you use and the device identifier (or 'UDID'). Additionally, each time you use the Services, we automatically collect information regarding the type of web browser you use, your operating system, your Internet Service Provider, your IP address, the pages you view on our sites, the time and duration of your visits, crash logs and other information relating to your use of the Services. "[19]
Personal data collected by the app	Policy is transparent about some personal data that are blockchain system specific like Wallet ID or app specific like account activity information without disclosing that the personal data is stored on the blockchain.	"Which personal data we process; ... Details concerning your transfers of cryptocurrency tokens, including IOTA tokens, insofar as these are publicly viewable on the cryptocurrency platform concerned."[20]
Personal data on blockchain	Policy explicitly states that personal data is stored on the blockchain.	"In certain circumstances, in order to provide you services of MediBloc, it may be necessary to write certain personal data, such as your cryptographic signatures onto the blockchain; this is done through a smart contract and requires you to execute such transactions using your wallet's private key."[21]

[15] https://horizen.global/privacy/
[16] https://gnosis.io/privacy-policy
[17] https://ost.com/privacy
[18] https://solve.care/docs/solve-care-website-privacy-policy/solve-care-website-privacy-policy.pdf
[19] https://horizen.global/privacy/
[20] https://www.iota.org/research/privacy-policy
[21] https://docs.medibloc.org/PrivacyPolicy_ENG.pdf

4.5 Portability

Table 5: Encoding Scheme for Portability

Code	Description	Example
None	This right is not covered.	NA
Very brief	Policy covers the right of portability in the list of data subjects rights that are respected.	"GDPR gives users the following rights: • Right of erasure (right to be forgotten) • Right of rectification • Right to be informed • Right of access • Right to restrict processing • Right to data portability • Right to object • Right not to be subject to automated decision making • Right to complain to a supervisory authority"[22]
Detailed	Policy gives details about portability including other controllers or technical feasibilities etc.	"If we process your personal information based on a contract with you or based on your consent, or the processing is carried out by automated means, you may request [in terms of GDPR] to receive your personal information in a structured, commonly used and machine-readable format, and to have us transfer your personal information directly to another 'controller', where technically feasible and once our platform interface allows for the 'exportation' of such data. In this connection, OCNEX is committed towards creating a robust function ensuring data portability in due course. Without prejudice to the aforesaid, data portability will be prohibited if the requested migration of said data adversely affects the rights and freedoms of others. A 'controller' is a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of your personal information."[23]

4.6 Data Retention

Table 6: Encoding Scheme for Data Retention

Code	Description	Example
None	This right is not covered.	NA
Vague statements	Policy says that they keep personal data if necessary. No time information or condition is provided.	"We also erase your Personal Data according to your request and if further storage is neither required nor permitted by applicable laws"[24]
Exact conditions	Policy explicitly states the exact period and/or conditions for data retention.	"If you contact us via email we will keep your data for 12 months; • your technical usage information for 12 months; • data on your use of our Website and Lisk Chat for 12 months. You can close your Lisk Chat account at any time. When you close your account, we will delete all of your personal data (and all of your chat history) within 90 days of you closing your Lisk Chat account."[25]

[22] https://www.horizen.global/privacy/
[23] https://support.ocnex.io/hc/en-us/articles/360018860651
[24] https://www.iota.org/research/privacy-policy
[25] https://lisk.io/privacy

4.7 Transfer of personal data to third countries or international organisations

Table 7: Encoding Scheme for Transfer of Personal Data

Code	Description	Example
None	This right is not covered explicitly.	NA
No DLT	Policy states that data is shared with third parties, countries/organisations for legal or marketing purposes without mentioning nature of Distributed Ledger Technology.	"A transfer of data to offices in the countries outside the European Union (so-called 'third countries') takes place when: it is necessary to execute your orders (e.g. payment orders, billing of credit card payments); it is necessary to fulfill our legal and contractual obligations towards you; it is required by law (e.g. tax reporting obligations); you have given us your consent or in the context of data processing in the order."[26]
Should not share	Policy states that they should not share data with third parties.	"Personal data should never be transferred outside of the European Economic Area."[27]
DLT	Policy states that DLT leads transfer of data to third countries due to its very nature.	"HOWEVER, WHEN INTERACTING WITH THE BLOCKCHAIN, AS IT IS A PUBLIC DECENTRALIZED NETWORK, WE WILL LIKELY NOT BE ABLE TO PREVENT EXTERNAL PARTIES FROM PROCESSING ANY PERSONAL DATA WHICH HAS BEEN WRITTEN ONTO THE BLOCKCHAIN. IN THESE CIRCUMSTANCES WE WILL USE OUR REASONABLE ENDEAVOURS TO ENSURE THAT ALL PROCESSING OF PERSONAL DATA HELD BY US IS RESTRICTED, NOTWITHSTANDING THIS, YOUR RIGHT TO RESTRICT TO PROCESSING MAY NOT BE ABLE TO BE FULLY ENFORCED."[28]

4.8 Data Minimisation

Table 8: Encoding Scheme for Data Minimisation

Code	Description	Example
None	This right is not covered explicitly.	NA
Brief	It is briefly stated that minimum personal data is collected.	"Processing of your data is carried out by our Company following the principles of lawfulness, fairness, transparency, and always adhering to the intended purpose of data processing, the principle of data minimization, accuracy, limited data storage, data integrity, confidentiality and accountability."[29]

4.9 Right of Access

Table 9: Encoding Scheme for Right of Access

Code	Description	Example
None	This right is not covered explicitly.	NA

continues on next page

[26] https://www.breaker.io/privacy
[27] https://s4fe.io/Data-Protection-Policies.pdf
[28] https://gnosis.io/privacy-policy
[29] https://genesis.vision/privacy-policy.html

continued from previous page

Code	Description	Example
Very brief	Policy covers the right of access in the list of data subjects rights that are respected.	"GDPR gives users the following rights: Right of erasure (right to be forgotten) Right of rectification Right to be informed Right of access Right to restrict processing Right to data Right not to be subject to automated decision making Right to complain to a supervisory authority"[30]
Brief	Policy says that personal data is provided in a machine readable format or structured way.	"Where the legal basis for our processing is your consent or the processing is necessary for the performance of a contract to which you are party or in order to take steps at your request prior to entering into a contract, you have a right to receive the personal information you provided to us in a structured, commonly used and machine-readable format, or ask us to send it to another person."[31]
How/Why	Privacy policy states not only access right, but also gives details about how or why the personal data is processed	"(Data subjects have) The right to request access to your Personal Information and to obtain information about how MediBloc processes it""[32]
Detailed	Policy states not only the access right, but also details about usage and sharing of personal data.	"All individuals who are the subject of personal data held by S4FE AG are entitled to: • Ask what information the company holds about them and why. • Ask how to gain access to it. • Be informed how to keep it up to date. • Be informed how the company is meeting its data protection obligations. If an individual contacts the company requesting this information, this is called a subject access request. Subject access requests from individuals should be made by email, addressed to the data controller at email address. The data controller can supply a standard request form, although individuals do not have to use this"[33]

[30] `https://www.horizen.global/privacy/`
[31] `https://gnosis.io/privacy-policy`
[32] `https://docs.medibloc.org/PrivacyPolicy_ENG.pdf`
[33] `https://s4fe.io/Data-Protection-Policies.pdf`