EUROPECHAIN
BY ZAISAN

GDPR COMPLIANCE POSITIONING

EXECUTIVE SUMMARY

Europechain supports web3 projects in being compliant with GDPR by providing a blockchain infrastructure that incorporates various GDPR compliant measures such as contractual architecture, data protection impact assessments, informing data subjects, privacy enhancing technologies, and consulting and assistance with compliance.

Europechain requires all contracts that include data processing to fully comply with GDPR and establishes controller-to-processor and processor-to-subprocessor data processing agreements. Europechain also requires dApps to provide information on their data processing and requires them to conduct a DPIA. Standard privacy texts are provided for dApps to include in their privacy statements to inform data subjects.

In addition, Europechain deploys privacy-enhancing technologies, registered Data Protection Officers, and dApp development tools that ease the use of deletable data. Consulting on standards and products, as well as assistance with DPIAs, is also available. Europechain also addresses regional deviations in GDPR implementation laws.

Overall, Europechain provides a comprehensive framework for web3 projects to ensure GDPR compliance in their data processing activities.

COLLABORATORS

JETSE SPREY
Chief Legal Officer

RHETT OUDKERK-POOL
Chief Executive Officer

CONTENTS

THIS IS AN INTERACTIVE PDF. CLICK ON A TITLE TO JUMP TO THE CORRESPONDING CHAPTER.

01 INTRODUCTION

This positioning paper describes the way Europechain public blockchain aims to support its projects in being compliant with GDPR and EU data regulations. While blockchain technology is still in its early stages, and this paper must remain a living document to adapt to new regulations, we base our principles on the long-standing European data protection tradition and GDPR basics. By making fundamental design choices that align with these principles, we can remain compliant and withstand policy changes that may impact other areas.

These fundamental principles, however, do require most blockchains to adapt thereto. GDPR compliance requires a certain level of centralisation. That "certain level" of interference with the blockchain, is obviously a threat to the immutability of the blockchain. While the consensus at the inception of blockchain technology was that only fully trustless decentralised networks can be considered blockchains, we believe that a decentralised blockchain with certain centralised elements is a stronger and better base to build enterprise-grade projects on.

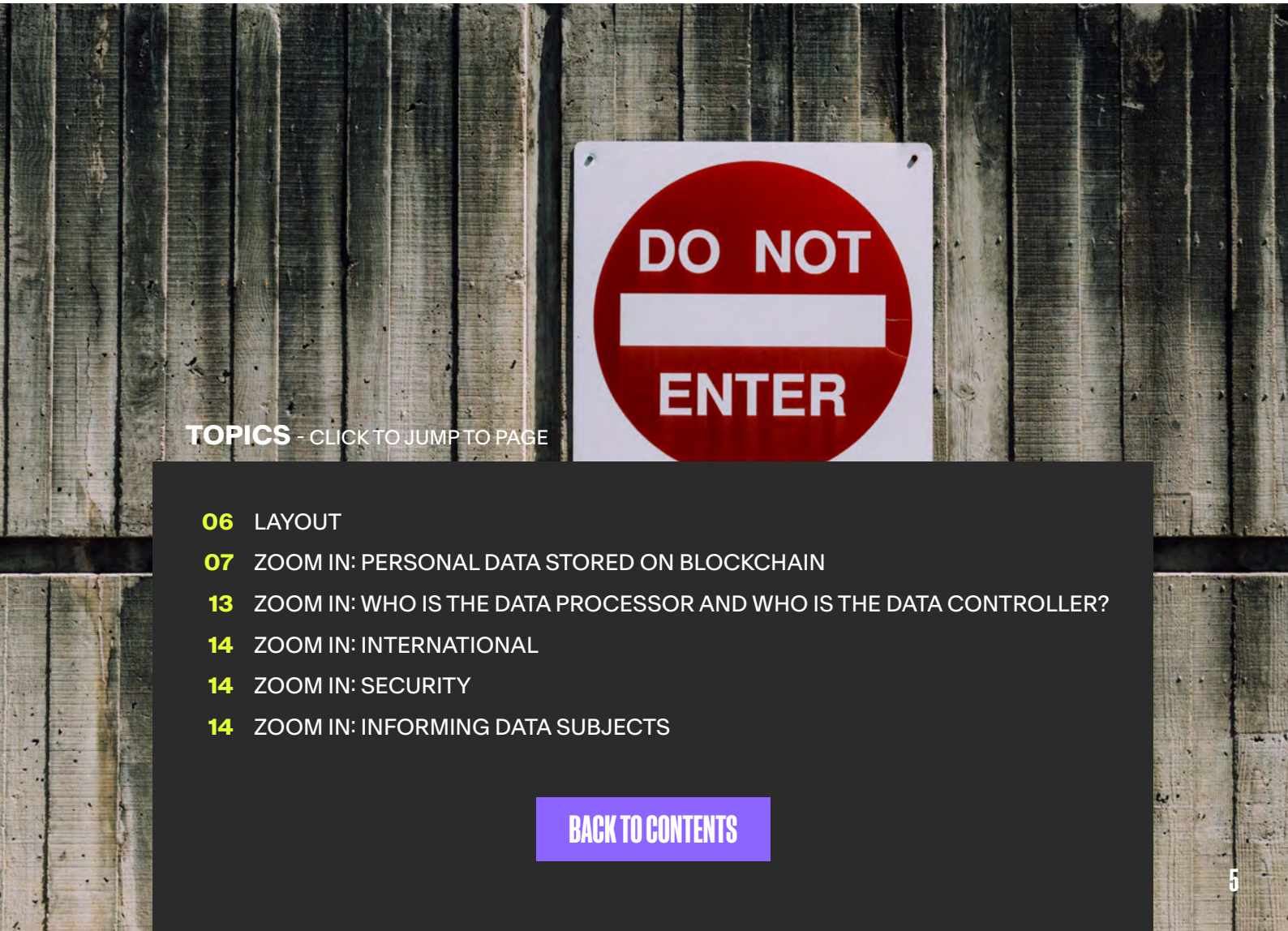
The only centralised elements are the elements strictly necessary to comply with the GDPR. Those will be detailed below. For now, it suffices to clearly state that meddling with any on-chain data by this central entity is not in any way included in the governance of Europechain, nor is it technically possible.

To ensure compliance with GDPR, each dApp running on the Europechain public blockchain will have to pass a Data Protection Privacy Assessment (DPIA). We will also provide additional services, such as monitoring for compliance, offering explanations of requirements, and obliging dApps to use privacy-enhancing technologies where necessary.

While this paper focuses on Europechain's public blockchain, other bespoke blockchains, private chains, and BAAS options may rely on it for guidance. However, each must be assessed individually to determine their privacy elements and establish the necessary documents and organisation.

02 HIGH LEVEL DATA PROTECTION ANALYSIS & MEASURES

This chapter discusses the tension between GDPR compliance and blockchain technology, highlighting the need to minimise personal data stored on-chain and to ensure appropriate safeguards are in place. This equalises to Europechain's approach of having EU-based block producers with relevant data processing agreements.



TOPICS - CLICK TO JUMP TO PAGE

BACK TO CONTENTS

LAYOUT

The GDPR considers all data that can be backtracked to a human, personal data. All data linked to a blockchain account may, therefore, be personal data. There is a natural tension between blockchain technology that stores some data forever and the GDPR that leans heavily on mutability: “the right to be forgotten” as its most outspoken feature in that respect.

This means that we should minimise the storage of personal data on-chain, even if encrypted. Encryption has a risk that future techniques may break it, while the blockchain will be there forever. The personal data needed to run a dApp can often be stored off-chain and shared with the chain. Such off-chain data will be encrypted and can be controlled. It can be altered and deleted. It is fully mutable data and in that sense comparable to any other data stored in any other database. GDPR compliance regarding that data will be “business as usual”.

However, the data that will be stored in a decentralised manner is an element to be taken into consideration. Exporting data out of the European Union is a big issue. Public blockchains (EOS, Telos, Bitcoin, Ethereum) work worldwide. Under the GDPR, this is not impossible but ‘appropriate safeguards’ should be in place. For instance each block producer may have to conclude a data processing agreement with each dApp that runs on the blockchain. That is why the Europechain will be unique in that it ensures that the block producers are all based in the European Union and have concluded relevant data processing agreements. This resolves these issues and contributes to a GDPR compliance supporting blockchain.

In the next paragraphs we will zoom in on matters as: “Who is the data controller and who is the data processor, security and information rights. Let’s look at the actually stored data first.

ZOOM IN: PERSONAL DATA STORED ON BLOCKCHAIN

Personal data that needs to be stored on the blockchain itself are:

- Public keys
- Account name
- Transaction details
- Hashes/transaction hashes
- Data in memo fields
- Tokens owned, staked, used for votes, etc
- Accounts with whom the account interacts
- Timestamps
- (Airdropped) tokens
- Possible other personal data

To avoid any misunderstanding: an account name or a public key is considered personal data, even if it seems impossible to identify an individual using this public key. However, this is a legal grey area. For the sake of compliance and remaining future proof we will presume public keys and account names are personal data.

The on-chain information can never be deleted or altered. Question is if that's a problem. That question is being addressed hereunder.

LEGAL GROUNDS FOR PROCESSING

Article 6 of the GDPR provides six legal grounds on which a data controller may process personal data. Without one of these grounds, processing is forbidden. In our analysis we will rely heavily, on two grounds regarding the storage of data on the blockchain: the execution of a contract and the ground that is called "legitimate interest".

Please note that off-chain data is not immutable. It can be deleted at will by the dApp, even if the blockchain would point to such data or contains a hash of such data (provided that it shall be a one-way hash). Which is why off-chain data will not be debated in this document.

Below we sum up the grounds and discuss their feasibility.

01 CONSENT

We could require consent for all account holders. There are many issues though, regarding consent. To name one showstopper: it must be possible to revoke consent. Following that, the controller must end processing which means deleting the personal data, which is impossible on the blockchain. Another important issue is that consent needs to be freely given. If a data subject gives his or her consent because he or she needs to give it in order to get his or her tokens, that is not a freely given consent.

02 EXECUTION OF A CONTRACT

One may process the data subject's personal data, as far as such processing is necessary to prepare for or to execute an agreement with the data subject. The account holder will enter into an agreement with Europechain and in order to execute that agreement Europechain needs e.g. the account name. For each of the data subject's data we will analyse whether this ground is feasible. The issue here will be the eternity of the blockchain versus the impermanence of agreements. Currently the general view is that agreements cannot be eternal. However, part of the agreement is the immutability of the blockchain. Which means that, in a way, for executing the agreement Europechain will need perpetual storage. In that sense an agreement regarding the blockchain has some eternity in it.

One might argue that the agreement lives on regarding that specific element. If that is the case, storage of the data on-chain is necessary to execute the agreement and this ground is applicable. One could also argue that each transaction on the blockchain is being executed by the parties with the immutability of the blockchain as an implied condition. Therefore, immutability is part of the agreement. And therefore, eternity is part of the agreement.

03 LEGAL OBLIGATION

There are currently no legal obligations to store data on the blockchain. This may change however, given the obvious advantages for e.g. public registers to be stored on the blockchain. For now compliance with a legal obligation is not a feasible ground.

04 PROTECTION OF VITAL INTERESTS

In matters of life and death one may sidestep lack of other grounds. This is obviously not a feasible ground to store data on the blockchain.

05 CARRYING OUT A PUBLIC TASK

This could be a valid ground for processing by governmental agencies. E.g. to ensure payments to. But for now, there aren't any tasks that require blockchain yet.

06 LEGITIMATE INTEREST

The final is the legitimate interest ground. This is an important ground. A controller may process personal data if one has a legitimate interest and the interests of the data subject do not prevail. Running a blockchain is a legitimate interest. We will provide extremely important digital infrastructure to society. Also the individual data subject does not operate in a vacuum. Where such data subjects may not like certain data stored on-chain, many, many others will rely heavily on the immutability of the blockchain for their income, to prove their possessions and for other material aspects. Deleting only one personal item, will render the blockchain at the cost of possibly enormous damage to the other users.

The question to be answered is that given the above, is it possible that the interests of the data subjects prevail? To address that question, we need to perform a balance test in which we balance the interests of the data subject in deleting his or her personal information against the importance of running a blockchain. If the balance tilts towards deleting, this means storing such information on-chain is not feasible. This balance test has to be conducted in respect of each of the datasets stored on the blockchain.

Regarding the balance test: the more intrusive the information stored is, the greater the interests of the data subject are in the balance test. And vice versa. The legitimate interest on the other hand has a continuously great weight: having to delete information on the blockchain means at the very minimum a hard fork and doing that, if even possible, would mean the end of the concept of immutability that is the basis of blockchain and the futures built and to be built on it.

Generally speaking, on top of that there are two important further nuances regarding the data subject interests. Firstly, even a hard fork doesn't mean the data is not available anymore. Anyone could have made a copy of the pre-fork blockchain and start publishing the information again.

This also touches on the second nuance. If one publishes personal information on the internet in general, deleting it doesn't mean it goes away. Millions of people could have made copies and started redistributing again. Deleting means making access to data more difficult. Which is important, surely, but it doesn't fully stop the availability of that data. Finally, not the full blockchain will be replayed each time. Older data will not be lost but will be harder to access over time.

Now let's take a deeper look at the types of personal data that has to be stored on-chain and how they should be viewed in the framework of these regulations.

BALANCE TEST TYPES OF PERSONAL DATA STORED ON-CHAIN

PUBLIC KEY/ACCOUNT NAME

The public key and the account name only mean that a person (which may or may not be known) has an Europechain account and has performed certain activities on the chain. That information in itself is not very intruding information. Millions of people will have such an account. But even in the first days of Europechain, when accounts will be few, the fact that one has an account on a blockchain that aims at compliance (or on many other blockchains for that matter) will not be intrusive data. An individual does not have a great interest in deleting that. The balance will tilt towards the blockchain and all concerned are entitled to refuse to delete public keys.

TRANSACTION DETAILS

The transaction details may include a great variety of data. An important example are the XEC tokens, Europechain's native token, that the account holds. Data generated by dApps and stored on the blockchain could widely vary. It can include, by way of example, ownership of certain goods, likes in a social media environment, ratings etc. etc.

For all of this data a balance test is required. Regarding the dApp data, such a balance test will be conducted before the dApp stores any data and will be part of the onboarding procedure of any dApp. However, the XEC that an account holds is not part of any onboarding process. It is native to the blockchain. Such an amount may be sensitive information, with the sensitivity being a function of the amount.

First of all, the balance test needs to take into consideration that this is a blockchain. The blockchain is always transparent, as is the combination of an account and the tokens such account holds. This is also the case with any other blockchain, such as Bitcoin or Ethereum. Without such basic transparency there is no blockchain, no digital money, or other digital assets. Given that storing such data is core to the blockchain, it is clear that deleting them would compromise the entire blockchain. If the blockchain is compromised, all XEC or all other account holders become compromised and may even lose their value. The balance test will therefore tilt in favour of continuously processing (storing) such data.

HASHES/TRANSACTION HASHES

The one way hash that is used is a one-way mirror. Meaning that with the hash one can never reconstruct the original data but that with the original data one can prove that the hash reflects the original data. Therefore hashes as such are, similar to the public key, data that are not very sensitive in itself. It is just the data that is hashed that may contain sensitive information but those data are not stored on-chain.

ACCOUNTS WITH WHOM THE ACCOUNT INTERACTS

Hashes and accounts with the person interacting and timestamps are metadata of the interaction. Timestamps and hashes as such, as isolated data, don't mean anything. Accounts with which a person interacts, however, may, even if we look at them as such, isolated from any other personal data, be problematic. An example of this may be the interaction with accounts of medical facilities.

That's why we should assess each professional account and decide whether interaction with such an account - as such - may cause privacy issues. If the answer is yes, additional techniques must be used. Transactions may be relayed through an identity provider that bundles transactions and in doing so masks the identity of the accounts behind it. This, however, raises serious issues. Rather than trust in the blockchain, trust needs to be vested in such providers. Another solution may be the use of temporary public keys that the user stores encrypted in his or her off-chain database.

DATA IN MEMO FIELDS

The data subjects may, and sometimes are required to, send information with any transaction in some data fields. That information is being stored on-chain. This information may contain any data about anybody. Therefore this field is an area of concern for the blockchain. One does not know which data will be entered there. Europechain will provide instructions to the dApps which data to ask for, Europechain will further warn each of the account holders not to enter sensitive information, will oblige them not to do it, and will finally hold any of those data subjects liable in the event they still enter such information.

Of course, at the end of the day, one cannot stop sensitive information being stored but given the warnings and the obligations of the account holder, it seems that, at least where the account holder's own information is concerned, the interests of the account holder regarding deleting sensitive data can hardly be called "legitimate". Where the account holder publishes information regarding other data subjects, this is more complex. We believe, given the steps described here, that the interests of the blockchain still prevail but there is a certain element of risk. We are working on solutions that, e.g., limit the size of the dataset and/or require a certain format.

COMBINATIONS OF DATA: DATA MINING

Data mining may be used to find patterns that may lead to profiles or information that is sensitive. Data mining can be used to try and find the account holder. Finding the identity of the account holder may be possible by combining data from various resources. This is just another, important, incentive to store as much off-chain as possible. However, given the small data set that we will need as a minimum, we also presume the on-chain data in itself will not be the issue here. If the on-chain data are instrumental in mining sensitive data, this might become an issue however. Bundling and encrypting may, once proven, offer solutions.

ZOOM IN: WHO IS THE DATA PROCESSOR AND WHO IS THE DATA CONTROLLER?

Under the GDPR data subjects must know whom to address to exercise their rights. Data subjects must know who decides what happens with their data, the authorities must know whom to address, etc. Most of the obligations under the GDPR are linked to the "controller".

The data controller decides what happens with the personal data and how that will happen. There could be more than one controller, which is understood as joint-controllership. The joint controllers have to let the data subject know which controller is responsible for which part of the processing. They have to make arrangements between each other. One has to focus on each and every use that's been made of personal data. Each processing activity regarding personal data must have at least one controller but may have multiple as joint-controllers.

A dApp provider that provides services through a dApp and stores user data and interacts through the dApp with their users, decides what happens with such data and, by choosing the particular dApp and the Europechain ecosystem, how that happens. Therefore a dApp provider will generally speaking be the data controller.

On the base layer, the system that Europechain provides, where we store personal data there is no dApp provider. This is the layer that interacts most with the data that is stored online: the accounts, public keys, transaction hashes inter alia.

There it gets complicated, given the decentralised nature of the blockchain. If in a decentralised situation where, like on the EOS, 15 out of 21 block producers (validators) decide what happens to the personal data, no one can tell who actually "rules" the blockchain. In that event either none of the block producers is controller or all of them are. Given the fact that there cannot be use of someone's personal data without a controller, the current idea is that all block producers of a blockchain are controllers. That is extremely complicated.

We have solved this issue. Zaisan B.V. will be the controller and the block producers will be data processors on the base layer (the main system). Where the dApp providers (or possibly even their clients) are controllers, Zaisan B.V. will be the processor and the block producers will be subprocessors.

ZOOM IN: INTERNATIONAL

By having all nodes and block producers in the European Union, we have ensured that no personal data of European Union citizens leave the European Union. Block producers may also be based in Norway, Iceland or Liechtenstein, the countries that belong to the European Economic Area.

Further we will ensure that ownership is predominantly European as well. Since Zaisan B.V. will select the block producers, this will be easy to manage. As for dApps of companies based outside of the European Union, we will provide the GDPR required representation services.

ZOOM IN: SECURITY

The blockchain and the data on it is public. It might be possible to encrypt and/or hide some of it but given our choice for a very limited data set, we do not believe that will be necessary.

The off-chain databases contain the data. Their encryption and protection will be assessed and brought up to standards continuously.

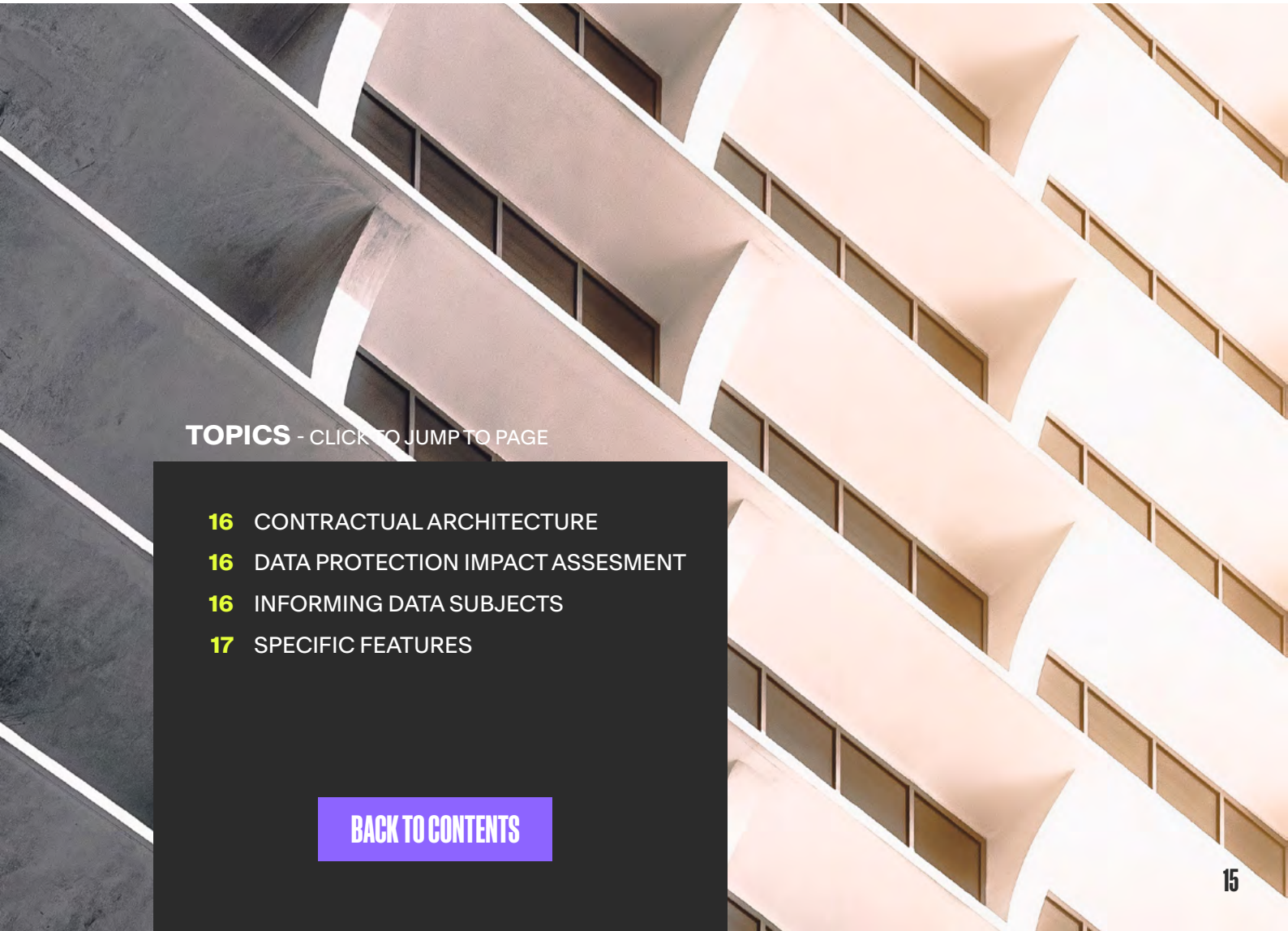
As for security: the authenticity of the data is extremely well ensured. That is the basis of the blockchain. Tempering with the data is just not possible. The on-chain data is public. There are no security issues regarding the confidentiality there since they are already public. The off-chain data is encrypted. The strength of the encryption defines the quality of the security.

ZOOM IN: INFORMING DATA SUBJECTS

We will inform all users when they open an account on the Europechain. In the event that the users do not register to interact only through the dApp provider, we will require the dApp provider to inform the users.

03 ORGANISATIONAL GDPR ARCHITECTURE

The measures we mentioned in the analysis above have been implemented as set out below. It is important to emphasise that all of these implementations are based on current views and current regulatory environment. We do not believe the basis to change but we definitely do not rule out specific regulations that might influence the set up.



TOPICS - CLICK TO JUMP TO PAGE

BACK TO CONTENTS

CONTRACTUAL ARCHITECTURE

In all our contracts that include data processing we will require full compliance with the GDPR. Zaisan B.V. will be the controller and the block producers will be the processor regarding system processing (as detailed above). We will conclude controller-to-processor data processing agreements (DPAs) and, as the case may be, processor-to-subprocessor DPAs. Contractually this means that access to the blockchain must be restricted to those dApps that have concluded such an agreement.

The privacy contracts will be incorporated in the Europechain's standard contracts. Compliance with the contracts may be enforced by blocking the dApps account in the event of non-compliance.

DATA PROTECTION IMPACT ASSESSMENT (DPIA)

The dApps will, inter alia, need to decide which data they will use, how long such data should be stored, how to implement any of the data subjects' rights and how to secure those data. We will require the dApp to provide that information. Based on that, Europechain may require the dApp to conduct a DPIA. We will assist where necessary. We may also require a third party legal opinion that the dApp is no threat to the integrity of the blockchain from a data protection point of view.

INFORMING DATA SUBJECTS

Regarding its processing, Europechain shall provide standard texts that the dApps must introduce in their privacy statement. The dApps shall have to inform the data subjects (their users) regarding the relevant elements of their processing.

SPECIFIC FEATURES

The following features and services will be deployed as well:

- Privacy enhancing technologies that use ephemeral public keys to interact on the blockchain representation for out of the EU dApps;
- Official history nodes filter for GDPR compliance. While all the transaction history is available to technically savvy people who are able to view the blockchain, history nodes which back block explorers are the popular way of viewing blockchain history. By sponsoring official history nodes, we can filter access to privacy sensitive information for the vast majority of users.
- Consulting and assistance with Data Protection Impact Assessments. We may safely presume that in a lot of cases such DPIA shall be necessary, given the new technology used.
- Registered Data Protection Officers.
- dApp development tools that ease the use of deletable data.
- Consulting on standards and products. Like CNIL paper, PIA tools and Priveos which give DApp developers additional tools for GDPR compliant applications.
- There are regional deviations on the GDPR in the local implementation laws, that make things either more difficult, or sometimes a bit easier. For example there is the German "Act to Adapt Data Protection Law to Regulation (EU) 2016/679 and to Implement Directive (EU) 2016/680" (DSAnpUG-EU) that states in Section 35: "If in the case of non-automated data processing erasure would be impossible or would involve a disproportionate effort due to the specific mode of storage and if the data subject's interest in erasure can be regarded as minimal, the data subject shall not have the right to erasure and the controller shall not be obligated to erase personal data in accordance with Article 17 (1) of Regulation (EU) 2016/679 in addition to the exceptions given in Article 17 (3) of Regulation (EU) 2016/679. In this case, restriction of processing in accordance with Article 18 of Regulation (EU) 2016/679 shall apply in place of erasure."