



## **ERASMUS+ - CHAISE Project - Module 2: Regulation, legal aspects and governance of Blockchain systems - Lecture 6: Blockchain and GDPR**

Frédérique Biennier

### **► To cite this version:**

Frédérique Biennier. ERASMUS+ - CHAISE Project - Module 2: Regulation, legal aspects and governance of Blockchain systems - Lecture 6: Blockchain and GDPR. INSA Lyon. 2022. hal-03873969

**HAL Id: hal-03873969**

**<https://hal.science/hal-03873969>**

Submitted on 27 Nov 2022

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

# **Module 2: Regulation, legal aspects and governance of Blockchain systems**

## **Lecture 6: Blockchain and GDPR**

**Frédérique BIENNIER**

Univ Lyon, INSA Lyon, CNRS, UCBL, Centrale Lyon, Univ Lyon 2, LIRIS, UMR5205, F-69621 Villeurbanne, France

## TABLE OF CONTENTS

<b>1</b>	<b>INTRODUCTORY PARAGRAPH .....</b>	<b>3</b>
<b>2</b>	<b>LECTURE NOTES .....</b>	<b>5</b>
2.1	GDPR .....	5
2.1.1	<i>Key principles .....</i>	<i>5</i>
2.1.2	<i>Obligations and rights.....</i>	<i>7</i>
2.1.3	<i>Implementing GDPR.....</i>	<i>8</i>
2.2	GDPR BACKED BLOCKCHAIN REGULATION .....	9
2.2.1	<i>Blockchain key principles facing GDPR .....</i>	<i>9</i>
2.2.2	<i>Implementing key GDPR requirements.....</i>	<i>11</i>
2.3	BLOCKCHAIN AS GDPR FACILITATOR .....	13
2.3.1	<i>Consent management.....</i>	<i>13</i>
2.3.2	<i>Data usage tracking.....</i>	<i>14</i>
2.4	CONCLUSION .....	15
<b>3</b>	<b>PRACTICAL EXERCISES .....</b>	<b>16</b>
<b>4</b>	<b>CASE STUDIES .....</b>	<b>18</b>
<b>5</b>	<b>QUESTIONS AND ANSWERS .....</b>	<b>19</b>
<b>6</b>	<b>MULTIPLE-CHOICE QUESTIONS .....</b>	<b>20</b>
<b>7</b>	<b>REFERENCES .....</b>	<b>23</b>
<b>8</b>	<b>SLIDES .....</b>	<b>24</b>



## 1 INTRODUCTORY PARAGRAPH

In this second module, we focus on the way blockchains are governed and regulated. In this sixth and last lecture, we focus on the way regulation regarding data protection, i.e. the GDPR, is taken into account while designing and using blockchain systems. This lecture takes advantage of the knowledge provided in the previous lectures, i.e. defining the blockchain context (lecture 1), the regulation and governance background (lecture 2), the organisation of the blockchain ecosystem (lecture 3) and the blockchain regulation (lecture 4). So, this lecture will mostly provide you some knowledge and skills related to the main GDPR requirements, the constraints related to the blockchain system and how the blockchain can be worthy used to manage and log both users' consents and the data usage operations.

Governing and protecting data is a major challenge to pursue safely the digital transformation. Of course, collecting data may take an important part in the development of the knowledge economy and there are numerous applications taking advantage of data science. Specific regulations are set to ensure privacy, limiting personal data usage to « fair usages » so that people privacy can be protected in both their real and virtual life. Let's now, focus on this data protection challenge. Are there specific security risks related to personal data? What may be the consequences of a privacy attack? To ensure privacy protection for European citizens, the General Data Protection Regulation Protection Act as been set in 2016 by the EU. Do you know the main requirements involved by this law? More precisely, how can you ensure that personal data are used fairly? How can you track the way your data are really used? Do you know how people and service providers manage consents?

All these questions and their answers are not so simple. Let's think and brain storm regarding these questions

As you can notice, describing data protection and identifying the way GDPR regulation impacts blockchain systems are not so simple. This requires first identifying key GDPR principles, i.e. understanding why and how this regulation is set, understanding the data protection key principles in a blockchain context. This lecture is designed to provide the necessary knowledge to understand and discuss key GDPR principles, the way it impacts blockchain systems and how blockchain can be used to manage key GDPR requirements, namely managing and logging consents and personal data due usages.

To sum up, this lecture addresses different learning objectives:

1. Data Protection Regulation context: focusing on the GDPR, you will learn its basic motivations, key concepts and the obligations and rights defined in this data protection act.
2. Blockchain regulation constrained by the GDPR: as an IT system, blockchains must also be compliant with GDPR requirements. Based on the key GDPR principles and on the blockchain ecosystem organisation, you will learn key principles and challenges to set GDPR-compliant blockchain systems / services.



- 
3. Blockchain as a tool to support GDPR implementation: Due to its intrinsic immutability characteristic, blockchain appears as a convenient mean to manage and log both consent and due usages so that both service providers and data providers can prove and check that data are fairly and actually collected, stored and used. You will learn how consents can be stored and how smart contracts can be used to manage access control and proofs of usage.



## 2 LECTURE NOTES

According to these learning objectives, this lecture is organised into three parts. First, we introduce GDPR, explaining its origin and introducing key principles so that obligations and rights can be precisely defined. Based on these GDPR key requirements, we analyse the key characteristics of blockchain systems to identify how GDPR compliant blockchain systems can be set, pointing out remaining challenges and debates. As said previously, blockchain can also be used as a support to manage consents, track data usages... In the last part of this lecture, we will show how smart contracts can be used to manage, log and prove « fair and authorised usages ».

So let's start now with the first part, i.e. introducing GDPR.

### 2.1 GDPR

#### 2.1.1 Key principles

GDPR has not been defined ex nihilo in 2016. Personal data protection has been initiated in France in 1978 by the "Informatique et Liberté" act, defining which kind of information can be collected, used and stored, which information cannot be used, how to declare files storing personal data... For example, information related to religion, politics, ethnic or trade union preferences or affiliations cannot be processed nor stored without specific authorisations. Since 1995 and the publication of the EU 95/46/CE directive, this privacy regulation has been expanded to the EU. This EU personal data protection regulation was quite different to the market regulation strategy deployed in the USA. To sum up, USA has a strict regulation for minors under 13 years and no constraints for older persons as the Federal Trade Commission considered that services with "unfair" or low privacy rules will not be used by customers. To deal with international constraints related to the EU 95/46/CE directive, the FTC has introduced the "Safe harbour" principles and certification so that US sites respecting this EU can be identified. Nevertheless, this international agreement was invalidated in 2015, as the level of protection provided by the USA is insufficient with regard to EU requirements. This invalidation has led to the development of the EU-US Privacy Shield, regulating data transfers from EU to USA. This agreement was also invalidated in 2020 as its protection level does not fit the EU requirements.

The EU GDPR has been defined according to this strong regulation background to fit the worldwide privacy challenge involved by the fast development of the Internet-based services, the development of the data economy, big data... This regulation, used as a model by other countries, has an extra-territorial scope. It means that personal data of a EU citizen must be protected world-wide. Personal data encompass all types of data related to a natural person: its name, address, phone number, its financial information (and transactions), health and genetics records as well as data related to its « digital life », i.e. images and video digitally stored, traces of the digital activities. The way these data are used by manual or automated processes (including business processes and big data / statistic processes) is regulated to ensure people privacy.

To manage data protection, GDPR introduces different roles. First, the subject is the physical person to whom the data are related.

- The subject is a natural person, in charge of defining its own privacy policy. To this end, the subject must explicitly consent to the data collection, storage and usage. This involves that the subject must be informed in a clear and synthetic way on the purpose of the potential processes, with who the data may be shared and for which purpose, the time period during which the data are stored... Nevertheless providing “informed consent” does not mean that the subject is fully aware of the risks, of the potential violation of its privacy policy... as consents are provided separately on one hand and as the current knowledge about privacy risks / digital hygiene is often rather limited (and sometimes non-existent).
- The data controller is a natural or a legal person representing the entity in charge of designing, running and controlling the processes using personal data. The data controller must be clearly identified and is accountable of the process. This why he must verify and may have to prove that the process is fully compliant with the legal requirements.
- The data processor is the entity in charge of processing the data on behalf of the data controller. As a consequence, it is not accountable of the process. It must simply ensure that security means are implemented to reduce security risks while processing / storing the data.
- The Data Protection Officer is in charge of implementing the GDPR. The DPO is a natural person in charge of managing globally the data security and the privacy protection. This means that the DPO must interact with the Information System Security Officer to ensure that security risks are clearly evaluated and that the necessary countermeasures are deployed to mitigate risks affecting the personal data. The DPO is also in charge of managing globally privacy protection and usage control, constraining data controllers while designing and managing processes.

As said previously, GDPR is inspired by works leading to previous regulation such as the EU directive 95/46/CE and international agreements between EU and USA. Protecting privacy involves a fair, lawful, transparent data processing. This means that data controllers are accountable of this requirement involving data minimisation, i.e. only the necessary personal data must be collected and stored for a given purpose, and a clear identification of the targeted usages. Although data archiving is allowed, other extra usages (i.e. usages which were not identified / are not necessary for the process) are forbidden. This purpose limitation involves that all potential usages must be mentioned and justified while the consent is obtained. Regarding the data archiving, un-necessary data must be deleted and only a time-limited storage is allowed, except for data used for scientific or public interest usages. Respecting these constraints is not enough to be compliant with the key principle of fair, lawful and transparent data processing. This means that data controllers and DPO must ensure that the data collection and processes fit legal constraints, i.e. that very sensitive data such as religion, ethnicity, trade union preferences... must not be collected nor processed without a legal derogation.

To ensure data accuracy, subjects are allowed to get access to their own data and to update them. As valuable resources and to increase privacy, a particular attention must be paid on data confidentiality and data integrity.

### 2.1.2 Obligations and rights

These GDPR key principles lead to different obligations for data collectors. First of all, the fair data protection involves that the data controller must get an informed consent of the person to which data are related. This means that this consent cannot be sum-up as “we are collecting data for due propose, click to continue”: subjects must be able to tune their privacy requirements according to the information on the usage purposes. This information must be provided in a synthetic and understandable way, describing both potential usages purposes and who may use the data according to these different purposes. Double opt-in (i.e. tick a box and confirm latter) have also been developed to provide a stronger “proof of informed consent”.

These requirements coupled to other initiatives such as Terms of Services Didn’t Read (ToSDR) has changed the consent collection mode: instead of having multiple pages very detailed and largely incomprehensible (which led de facto to approve without reading), templates structure uses by large families and allow to accept or refuse groups of purposes. Nevertheless, this may not be enough to ensure privacy as information on data processors and their other legal obligations such as the Cloud Act are often missing, leading to a risk against sovereignty.

Another important obligation related to the fair, lawful and transparent data processing is the development of an efficient data protection and security policy. As data controllers are accountable for the data processing, they are also accountable regarding the way data are protected. This means that setting an efficient data security policy is mandatory, including clear and consistent risks assessment and efficient countermeasure means implementation. Paying attention to the real-life consequences of any personal information disclosure, GDPR imposes a 72 hours maximum delay to notify interested parties about data thefts. We can note that this delay is very short compared to the 240 days representing the average delay of detecting intrusions...

Lastly, a Data Protection Officer must be appointed to manage and control the GDPR implementation.

GDPR equilibrates data controllers’ obligations with new rights. The potential extra-territorial protection allows transnational data transfer. This has led to specific agreements to support this extra-territorial competency counterbalancing other national less protective regulations. Paying attention to the complexity of distributed IT processes and infrastructure, GDPR grants data controllers the right to define precisely their accountable sub-contractors in order to define “responsibility chains”, so that each actor is accountable of its actions. Of course, this can be seen as a right (I can decide that I’m not accountable for my sub-contractors as I cannot fully control them) or an obligation (If you do not want to “pay” for actions your sub-contractors have done, YOU MUST specify clearly the co-responsibility chain and deploy means to show that you’ve done the job properly).

The main rights provided to data controllers are related to the allowed purposes. First, fitting the data economy development, GDPR legitimates merchant exchanges of personal data. This support new data-based business models and marketing strategies. Selling data to support targeted advertising favours prospecting and market development based on digital activities. Second, GDPR legitimates data collection for statistic purpose, provided that the statistic process is not discriminatory. Moreover, it is no more necessary to collect the subject consent if the process is related to an “essential interest”, i.e.



related to health, state interest or system security. This new right involves that data controllers must prove the “essential interest” of their process and log data usage to prove that the collected data are not used for any other purpose.

Regarding the subject, GDPR extends the rights of the EU directive 95/46/CE. Of course, any subject can get access to any data related to him/her whether the data was explicitly given or collected automatically (with or without consent depending on the type of purpose). This right is enforced as subjects must be informed of any data collection, including usage identification, motivations... and must provide clearly their consent for this data collection.

An important right granted to subject: the right to erasure. It means that non-anonymized data can be stored during a reasonable time and must be erased or archived in an anonymized way after this period. Another right, the right to be forgotten allows also to increase privacy.

Paying attention to the way users want to manage their “digital life” (and the associated data), the right of appeal is simplified, involving a single authority in charge of propagating the appeal along the global chain.

Lastly, due to the development of dematerialized processes, more and more documents are stored digitally. This means that the associated data and documents are stored digitally. This requires allowing subjects to get back their data and documents in an interoperable way.

### **2.1.3 Implementing GDPR**

Implementing GDPR requires appointing a Data Protection Officer in charge of advising data controllers about GDPR constraints and checking globally the GDPR implementation. First, data controllers have to document precisely data and processes, defining precisely the process purpose, the data used and the way data are processed so that they can provide the exact information to collect the informed subject consent. To improve data security and privacy, it is recommended to set a privacy by (re)design strategy. It consists in evaluating, from the initial design steps, the privacy impact of the processes. A particular attention is paid on the data security policy, identifying potential threats, vulnerabilities of the system and setting the adapted countermeasures to mitigate risks. Based on this analysis, processes can be redesigned, integrating the highest data security and privacy requirements.

We must note that data controllers may have to demonstrate the compliance with GDPR, logging data accesses and usages, identifying clearly the processes using them. Managing data security requires integrating human-related risks, that may lead to intrusions in the system.

Focusing on legal aspects, data controllers must define precisely contracts with their sub-contractors so that clear responsibilities can be identified, limiting appeal risks.

As the GDPR constraints process organisation, may limit the data usage and consequently may impact some business models, implementing GDPR is not only a matter of appointing a Data Protection Officer, it requires the involvement of the corporate governance, including top management. Business departments and IT department must also be involved in order to precise exactly the requested data and process purposes and even re-design processes to fit GDPR implementation constraints. A particular

involvement of the Information System security Officer is needed in order to refine and precise the data security policy, improve the security processes in order to track and report more efficiently potential attacks, intrusion and data thefts and improve the internal processes data access control to allow only accesses and usages fitting the consents provided by subjects. This must be done in coordination with the data protection officer who is responsible of managing the global protection consistency related to the GDPR implementation.

This means that implementing GDPR in an organization is not simple. Dedicated surveys propose best practices for the different groups of actors regarding processes, protection and security objectives, the way security processes can be designed and implemented or providing a legal framework to cope with the GDPR requirements.

The implementation of GDPR implies a significant change in data management habits. Every action involving personal data must be logged so that data usage can be tracked and proven. It is necessary to set up awareness actions for users to explain the changes induced on the processes, to enable them to improve their IT hygiene to avoid undue access or intrusions and to ensure that all actions are logged. Planning regular audit controls are also necessary to ensure that all security and data protection processes are implemented efficiently and to improve data protection.

## **2.2 GDPR Backed blockchain regulation**

So, after introducing GDPR, let's now pay attention on the way GDPR can be implemented in blockchain systems. To this end we will first focus on blockchain key concepts and the way they can match or not GDPR requirements before showing how GDPR key requirements can be implemented.

### **2.2.1 Blockchain key principles facing GDPR**

As we have just seen GDPR implementation relies on key roles identification such as data controllers and data processors, storing and consuming personal data, and data subject, i.e. the natural person to whom data are related. Under the responsibility of the data controller, using personal data involves defining precisely the process purpose to ensure a faire, lawful and transparent data processing while subjects are allowed to get access, modify and delete their personal data.

As a technologic object, Blockchain systems can be seen as neutral systems providing an immutable and safe storage of blocks storing P2P transactions. It means that there's only one process purpose (immutable storage) and that no change is allowed, which can be seen as opposed to data updating and data erasure requirements.

Focusing on the blockchain ecosystem, the variety of roles (validators, developers, users, investors...) make difficult the identification of the responsibility chain as all processes are heavily distributed. Moreover, the user pseudo-anonymity contravenes the accountability principle of the GDPR

So, implementing GDPR in blockchain systems requires analysing the way key principles can be deployed in such distributed systems.

The protection of data provided by the GDPR is based both on the identification of the objectives of the processes consuming this data and on the effective access to this data. A blockchain-based system can be seen as a simple tool for different uses. In this context, the objectives of the processes are rather related to the "application" services using the blockchain while the effective access control is more the responsibility of the blockchain system.

The definition of access control in traditional computer systems is based on elementary services called CRUD, namely Create / Read / Update (read to get the data and then write a new value replacing the previous one) and Delete a data / a record from a file or a data base. As a blockchain stores blocks, can we use these elementary services? Of course, a block can be created and read (retrieved) but the immutability property of the blockchain involves that blocks cannot be updated nor deleted. This is a major problem regarding GDPR implementation as subjects are allowed to modify and erase their data and may also be "forgotten".

This questions first on what can be stored in the blockchain. Should GDPR implementation lead to never store any personal information in a blockchain, and as a consequence make blockchain support unusable for classes of applications requiring a safe and immutable storage of personal data? How can a blockchain fulfill the data creation / access / update and erasure requirements involved by GDPR implementation?

In fact, elementary access control services must be redefined to fit blockchain systems characteristics. As said previously, a block including a transaction can be created and retrieved allowing to read its content. Considering the way how the update and deletion functions can be implemented, an adaptation is required as blocks are chained and changing the content of a block impacts the full chain consistency. To cope with the data updating requirement, a solution may consist in appending a new transaction / block with the updated content. By this way the blockchain may be used as an immutable storage of logged data, i.e. the blockchain contains all the different values of this data. Focusing now on the data erasure requirement, we can note that a digital data is deleted when it cannot be accessed anymore, i.e. its value cannot be used in any further computation. Data deletion does not mean that the system physically "destroy" / thrash the data, simply the data record is free and can be burnt to store a new digital data. By analogy with this analysis, any encrypted data for which encryption/decryption keys are lost becomes unusable and can therefore be assimilated to destroyed data. Implementing data erasure in a blockchain is then possible for encrypted data by setting a "burn" operation deleting the encryption/decryption keys associated to this data.

So, turning CRUD elementary services into CRAB services makes possible the GDPR implementation for blockchain-based systems, provided that data records stored in the blockchain are encrypted with independent keys.

Other key requirements of the GDPR are on one hand the data subjects and data controllers' authentication and on the other hand the protection of the digital activity tracking. These two requirements may be opposed to blockchain systems organisation as blockchain users are identified by the key they own and as all transactions (i.e. blockchain-based activities) are stored immutably.

Blockchain are known as anonymity preserving system as they use a pseudo-identity. Users can create and retrieve a transaction according to the associated key, i.e. something they own.

Let's first consider that the user storing a data in a blockchain is the subject, i.e. the person to which the data is related. It means that the exact subject authentication depends on the way the subject gets and manage his associated keys, i.e. depending on the wallet manager used by the subject. We can note that when encrypted data are stored in a blockchain, the subject storing the data in the blockchain can decide who can get access the data retrieval function by sharing or not the requested decryption key. When a subject uses a same key to sign different transactions, he may be re-identified and this leads to a privacy risks when different sources mixing these encrypted data are used.

When a blockchain is used as a certified and immutable storage mean, the blockchain user may also be an external process storing a subject personal information. In such a case, the blockchain user is associated to the process for which the associated data controller is accountable. It means that the blockchain user stores / retrieves / appends / burns transactions in the blockchain "on behalf" of the real subject. This involves that the blockchain can store immutably data creation / data append and data burn actions from the data controller who is then in charge of managing properly data encryption keys for the data user.

Paying interest on the blockchain activity tracking, this risk is related to the transaction retrieval. It may be possible to browse blockchain systems, extract transactions associated to a given pseudo-identity and make "cross-sourced data" privacy attacks. This is heavily couple to the way users manage their own wallets and their cryptographic keys.

### **2.2.2 Implementing key GDPR requirements**

Focusing on the blockchain ecosystem (as defined in lecture 3), we can identify different roles:

- Miners / block validators ought to be neutral regarding the data. They do not pay attention to the block content "semantic" as they just use it for cryptographic computations. As such they can be seen as GDPR data processors.
- Blockchain developers provide the technical means to support the blockchain internal processes. These blockchain processes are "neutral", i.e. they do not depend on the meaning of the content of the transactions / blocks they manipulate. As these processes do not consume personal data, developers are not aware of data usage. So they are not involved in key roles for the GDPR implementation.
- Blockchain service / application layers members: these actors use the blockchain system for a given business purpose. As such they are aware of the purpose of the process using personal data. This means that they may be associated to data controllers and take a part in the accountability chain.
- Blockchain investors: as they can take a part in the blockchain system governance, investors can also be involved while defining process purpose. Nevertheless, this coarse-grained purpose will



only guide service / application layers members or process developers. This is why investors are not seen as data controllers.

- Blockchain users: as we just said, the blockchain user is the entity storing / retrieving transactions in a blockchain. When the blockchain is designed as a technical component of an information system, the blockchain user is associated to the process that may store personal data in the blockchain, acting “on behalf” of the data subject. In such case, the user can be considered as a data controller from a blockchain interface point of view. As far as end-users are concerned, they can cope with the subject and data controllers’ role as they can store data related to them and decide freely to use the blockchain for a given purpose. In this last case, the key question is identifying if they got the necessary knowledge of blockchain characteristics and risks to decide “freely” to use it.

Data controller is a key role in GDPR implementation as it is the entity accountable of the faire, transparent and lawful personal data processing. For private and permissioned blockchain systems, there’s a clear identification of blockchain actors, of their role. The blockchain usage purpose is also well defined. This make possible the clear identification of data controllers as responsibilities are well defined for each consortium member. It is also possible to consider blockchain “data controllers” as subcontractors acting on behalf of business process related data controllers.

Regarding public blockchain, the distributed and collective data processing does not allow identifying clear responsibilities leading to unambiguous data controller role identification. Blockchain can be considered as a global process where end-users are responsible for deciding which information is stored in the blockchain, acting as “kind of” data controllers. This is why data controller role is still under debate.

Let’s now consider the GDPR key rights. Blockchain stores block in a distributed way. This increases data availability but also data security as different copies of the ledger may be hacked. This makes harder the necessary data security controls. It may make more complex to respect the 72 hours notification delay as intrusion detection is more complex. A last problem related to the blockchain distribution resides on the extra-territoriality, mostly for public blockchains. In fact copies of the blockchain can be stored world-wide under different legal frameworks, making harder the real control on transnational data transfers when several copies are dispatched. Whereas the blockchain distribution can be seen as a breaking force regarding GDPR adoption, on the contrary, the blockchain storage can favour transparency and data portability rights. As blocks are stored immutably, retrieval functions can be used to get access and extract relevant personal data stored in the blockchain. Of course, this limits the data updating and data erasure rights, unless CRAB services are set.

To sum-up, implementing GDPR in blockchain systems challenges for identifying clearly data controllers. It also constraints data due to the blockchain immutability property. Storing data in a blockchain means that data can be retrieved. This cope GDPR constraints for anonymous or immutable and public interest data (for example, a diploma certification may be considered as a public interest data). For mre sensitive data or the implementation of erasure right, this requires storing only encrypted data so that CRAB services can be deployed.

So, it sounds possible to implement GDPR in blockchain systems. Nevertheless, blockchain is still an immature technology with potentially new usages. This means that key questions are still under debate and that blockchain must be considered as a technical tool among others. Implementing GDPR compliant blockchain systems requires integrating the blockchain in the complete data processing architecture, defining clearly and precisely Blockchain usage purposes. Similar to other component of an information system, personal data involved in a blockchain must be minimized and a particular attention must be paid on the data “pre-protection” when it is impossible to use anonymized data: obfuscated data provides a minimal privacy protection while encrypted data can be used to manage properly CRAB services and increase privacy. But keep in mind that if the distributed organisation of the blockchain increases data availability, it may also be seen as a security vulnerability / threats as copies of the blockchain may be dispatched without much controls.

## **2.3 Blockchain as GDPR facilitator**

As GDPR requires a safe logging of the different consents and actions, blockchain technology can be seen as a convenient support to monitor consent collection and usages thanks to the immutable and safe storage feature blockchain provides. In this last part, we introduce some recent research work dealing with this opportunity.

### **2.3.1 Consent management**

GDPR empowers users with their personal data and privacy management by setting new obligations for the organisations and processes “consuming” or storing personal data: processing personal data in a fair and transparent mode requires informing the natural person to whom the data are related and collecting his consent for this data processing and monitoring the way these personal data are involved in running processes. As the data controller, in charge of a process consuming personal data, is accountable of the fair, transparent and lawful data usage. This means that the data controller may have to prove that data are collected and processed according to the collected consent. This leads to two key challenges, i.e. proving that an informed consent was collected and that personal data are accessed and processed only according to the pre-defined and agreed purposes. To meet these challenges requirements, a safe and immutable log storage feature is required, leading to study how blockchain can be used to provide the technical means to improve GDPR implementation.

First, let’s consider how a blockchain can be used to manage consents. Roughly speaking, a consent may be modelled as a set of access rules. Each rule is represented as a T-uple describing the subject, i.e. who will be granted or not a usage right, the object, i.e. the set of data for which the usage right is provided, the target usage, conditions such as time validity, and the decision part (grant / deny). This example picked from the Ontology-based Right Expression Language shows that an access right rule is modelled in a similar way. The key point consists in specifying GDPR adapted usages, paying attention to the access operation AND to the business process purpose to legitimate or not the personal data usage.

To define the process purpose, we can reuse the UCON<sub>ABC</sub> model (see Pretschner, Alexander, Enrico Lovat, and Matthias Büchler. "Representation-independent data usage control." Data Privacy Management and Autonomous Spontaneous Security. Springer, Berlin, Heidelberg, 2011. 122-140). This

model relies on a usage ontology to define rights that are associated with basic usage operations (i.e., Create, Read, Update, Delete), subjects who will get a usage right, objects which define the asset on which the usage right is granted, obligations associated to protection means and restrictions associated to time or environment constraints. We have proposed to expand this ontology to

- Integrate more complex data-related operations, to define more precisely the way data are processed, exchanged, replicated, and stored
- Integrate organizational knowledge to define the subject (a user, a group, or an organizational entity)
- Integrate business knowledge to define more precisely the usage context, specifying a process motivation, process purpose, and business scope related to business areas.

In order to prove that a consent has been collected, a blockchain-based system can be used. In such case, a consent is modelled as a P2P transaction linking the subject (i.e. the natural person to whom the data is related) AND the data controller (i.e. the entity responsible of the GDPR compliance management for a given set of processes). This time-stamped transaction can be stored immutably in a blockchain so that both subject and data controller can refer to it to prove what has been granted or not. Logging different time-stamped consents is also possible so that the subject can change its privacy requirements and the data controller can extract the exact time-stamped consent to allow or not the personal data processing.

As a consent may be considered as a sensitive data, systems often store the encrypted consent and / or its hash so that the blockchain record supports the “consent approval” proof.

### **2.3.2 Data usage tracking**

Blockchain can also be used to prove that data are used according to the approved consent. Different works have used smart contracts to implement access / usage rights. This provide an efficient support, allowing users to retrieve the smart contract derived from a given consent in order to check the precise usage rule and usage condition. In fact, the smart contract is used in a kind of “Kerberos” authorisation system: when a smart contract is fired, it provides a token to the data consumer to prove that the usage operation can occur while login the access operation. Despite its interest, such smart-contract based access control remains complex and a main risk is related to the way blockchain users are identified: if a cryptographic key is hacked, access right tokens can be transferred to unauthorized users.

To overcome this problem and ensure that sensitive personal data cannot be accessed without authorisation, other works propose to store encrypted personal data, using smart contract to transfer the necessary keys to allowed processes. By integrating several encryption processes (quite similar to the IKE protocol), this architecture leads to complex computations but there are reduced risks that a sensitive data can be used by unauthorized actors.

So, thanks to its immutability characteristics, blockchain systems can be seen as an efficient technical tool to support GDPR implementation. Different application services are defined to this end including Personal Information Management Systems, allowing natural persons to manage consistently their own personal information system, consent managers that can be worthy used by data controllers to prove



that their usages fit the provided consent and even access control systems, logging usage / access operations.

Most of these systems are based on private and permissioned systems, easier to manage and control and minimise the personal data they store so that no extra GDPR constraints are needed.

## 2.4 Conclusion

As we seen in this lecture, GDPR constraints blockchain implementation and at the same time GDPR implementation can take advantage of the blockchain properties. So, it's now time to conclude.

The EU GDPR adopted in 2016 has been applied since 2018. It provides a legal framework to improve privacy for EU citizens. It defines clearly new rights (as the authorisation of statistic process, transnational data exchange...) counterbalanced with obligations such as strict informed consent collection or logging usage and data accesses) for data consumers while empowering natural persons to manage their own information system privacy policy. This data protection regulation has initiated an extra-territorial control on privacy for EU citizens. Its key principles, fitting the digital transformation involving more and more exchange of personal data, have been reused by other countries to set their own extra-territorial data protection regulation.

Despite its interest, GDPR protection is limited by the end-users themselves as they may non-consistently consent to share, personal information with various and sometimes unknown actors, without paying attention on the process purposes.

Key questions are related to data disclosure, as this may be opposed to data controllers. Finding the "root cause" of data disclosure is not obvious and data consumers (i.e. the service providers consuming the data) must prove that they are not the cause of the data leaks.

We can note that GDPR was defined as a first step regarding the data economy protection: the new EU data governance act, approved in 2022 is designed for the different kinds of data.

Due to its intrinsic distributed organisation, blockchain can hardly cope with GDPR requirements, mostly regarding the identification of data controllers and data subjects. The definition of new CRAB elementary data manipulation services allows fitting the data access, logged data updating and even data erasure for encrypted data. Due to its safe and immutable storage ability, blockchain can be worthy used to store time-stamped consents or log data accesses thanks to smart contracts. By this way data controllers can manage efficiently proof of their fair, transparent and lawful usage of personal data.



### 3 PRACTICAL EXERCISES

This practical exercise shows how you can identify some blockchain GDPR regulation. The case study used in the different exercises from this module is based on a supply-chain / industry 4.0 case study.

Let's consider the organisation of a "producer to consumer food supply-chain". Different producers are involved in the food procurement and transformation. Each member of the supply-chain ecosystem can integrate its own suppliers in a "sub-supply chain". In order to eliminate wastes, the supply chain is managed in a Just in Time strategy. Increasing the product quality and the production transparency leads to track each product / transformation process so that consumers can be called in case of trouble.

Identify a GDPR challenges for this ecosystem.

To solve this problem, you need to identify

- The different GDPR actors involved
- The different kinds of personal data that can be involved in this system
- The personal information that may be used in the blockchain system

For each topic you need to ask some Who / What / For What / From where / Why / How questions

- The business-oriented ecosystem relies on the collaborative networked production organisation. As seen in lecture 3, this is a partner-centred organisation. Focusing on the blockchain organisation, identify some blockchain genesis hypothesis and their impact on the key GDPR actor definition
- Focusing on the system organisation, identify the different personal data it may include
- Identify which data can be stored in the blockchain.

Analysing the requirements shows that:

- The business-oriented ecosystem relies on the collaborative networked production organisation. As seen in lecture 3, this is a partner-centred organisation. Focusing on the blockchain organisation, we can say that the blockchain will be a component of the distributed system and may be organized in a private and permissioned way. To evaluate who may be the data controllers, we need to consider who owns the blockchain
  - a. The main stakeholder may be the unique owner: this happens if the main stakeholder provides the full blockchain infrastructure and constraints its partner to register their production in the blockchain. In such case, the main stakeholder must identify a data controller associated to the blockchain and the responsibility chain will consist in propagating data controllers responsibility among the different sub-processes



- b. The project may be launched as a common answer of all participants to regulation constraints / quality processes / main clients' requirements... In such case, all partners involved in the supply chain are founding members and may identify their own data controller involved in the blockchain interaction. In such case, the end-user will refer to the data controller to whom he sends its consent
- Tracking supply-chain and production processes may lead to store
  - a. various activity-related personal data such as location of vehicles (and workers), key production activities of an employee... This means that these data must be obfuscated before being stored in the system
  - b. Regarding end-user data, personal information can be reduced to purchase information (including the different products) and a client ID. These data are commonly used for statistics and marketing purposes. Extra personal information including contact information can also be stored
- Data stored in the blockchain are related to the different transactions among the supply-chain partners and the client. Consequently, only production activity and purchase information should be stored in the blockchain.



## 4 CASE STUDIES

### Agri-food NFT Case study

A group of agri-food enterprises want to set a NFT-based loyalty program associated to the product they sell. Each company will provide some “loyalty score” depending on the customer activity. These loyalty scores are managed by a dedicated entity. Each customer can apply for a given NFT attached to a rare “real product” provided that he gets enough validated loyalty score. These NFT are used to grant access to the product ordering. Identify key personal information that may be stored with the NFT to define GDPR requirements for the NFT blockchain system.

or

Choose an example of blockchain project and analyse it in a similar way as what was done in the exercise.

## 5 QUESTIONS AND ANSWERS

### Description

#### Question and Answer No.1

**Q:** Which kind of data is protected by GDPR?

**A:** Any data related to a natural person. It includes identification data financial data, health data, images and data related to the digital life including internet traces.

#### Question and Answer No.2

**Q:** What is the key principle of GDPR?

**A:** GDPR guaranty a fair, transparent lawful personal data processing.

#### Question and Answer No.3

**Q:** What are the elementary data manipulation service in a blockchain?

**A:** While traditional systems use the basic Creation / Read / Update / Delete (CRUD) operations, data stored in a blockchain uses Create / Retrieve / Append and Burn basic operations.

#### Question and Answer No.4

**Q:** Can you explain how data can be updated or erased in a blockchain?

**A:** Data can be updated thanks to the Append operation: the modified data is stored in a new time-stamped block this allows logging all values of a data. Data erasure is managed only for encrypted data. In such a case, the burn operation is used to delete the cryptographic keys associated to the encrypted data that must be erased. By this way, the stored data cannot be retrieved nor understood anymore.

#### Question and Answer No.5

**Q:** How can blockchain support GDPR implementation?

**A:** A blockchain can be used to store consents and report data usages thanks to smart contract. This allows proving that users have provided an informed consent and logging usages that are compliant with the consent



## 6 MULTIPLE-CHOICE QUESTIONS

### Multiple Choice question No. 1

**Q:** GDPR controls personal data usages in

**A:** both automated and manual processes

- Automated processes
- Manual processes
- Both automated and manual processes

### Multiple Choice question No. 2

**Q:** Who is in charge of managing globally a GDPR implementation in a company?

**A:** The Data Protection Officer - DPO

- Data Controller
- Data Protection Officer
- Data Processor

### Multiple Choice question No. 3

**Q:** Is it possible to implement a personal data erasure in a blockchain implementation?

**A:** Yes but only for encrypted data thanks to a “burn” operation

- No the blockchain provides an immutable storage so no data can be erased
- Yes, data erasure can occur in a blockchain
- Yes, but only for encrypted data thanks to a “burn” operation
- Core development evolution

### Multiple Choice question No. 4

**Q:** Who are the data controllers in public blockchains?

**A:** Not fixed yet, this is still under debate

- Not fixed yet, this is still under debate
- Miners
- Investors

### Multiple Choice question No. 5



**Q:** GDPR allows

**A:** any non discriminatory statistical process

- Any statistics process
- No statistics process
- Any non discriminatory statistical process

### Multiple Choice question No. 6

**Q:** The informed consent is given by

**A:** the subject

- The subject
- The data controller
- The data processor

### Multiple Choice question No. 7

**Q:** Storing consents in blockchain allows

**A:** Proving that a time-stamped consent has been provided by the subject

- Proving that the user has read and has understood the terms of service
- Proving that a time-stamped consent has been provided by the subject
- Providing the potential usages to the subject

### Multiple Choice question No. 8

**Q:** Blockchain users are

**A:** either data subjects or data controllers

- Data subjects
- Data controllers
- Either data subjects or data controllers

### Multiple Choice question No. 9

**Q:** Data controllers are identified

**A:** only for private permissioned blockchains

- For public and private blockchains
- Only for public blockchains



- 
- Only for private permissioned blockchains

### Multiple Choice question No. 10

**Q:** Smart contracts can be used

**A:** to implement usage-based access control

- To inform end-users that some of their data are used in a process
- To implement usage-based access control
- To generate on the fly adapted consents




## 7 REFERENCES

- <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
- [https://www.europarl.europa.eu/stoa/en/document/EPRS\\_ATA\(2018\)624254](https://www.europarl.europa.eu/stoa/en/document/EPRS_ATA(2018)624254)
- <https://www.eublockchainforum.eu/reports/blockchain-and-gdpr>
- <https://iapp.org/resources/article/blockchain-and-gdpr/>
- Humbeeck, A. V. (2019). The blockchain-GDPR paradox. *Journal of Data Protection & Privacy*.
- Data Governance act: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52020PC0767>
- Haque, A. B., Islam, A. N., Hyrynsalmi, S., Naqvi, B., & Smolander, K. (2021). GDPR compliant blockchains—a systematic literature review. *IEEE Access*, 9, 50593-50606.
- Truong, N. B., Sun, K., Lee, G. M., & Guo, Y. (2019). Gdpr-compliant personal data management: A blockchain-based solution. *IEEE Transactions on Information Forensics and Security*, 15, 1746-1761.
- Berberich, M., & Steiner, M. (2016). Blockchain technology and the GDPR-how to reconcile privacy and distributed ledgers. *Eur. Data Prot. L. Rev.*, 2, 422.




## 8 Slides



blockchain skills for Europe

# Module 2: Regulation, legal aspects and governance of Blockchain systems

## Lecture 6: Blockchain and GDPR



Co-funded by the  
Erasmus+ Programme  
of the European Union

2. REGULATION, LEGAL ASPECTS, AND GOVERNANCE OF BLOCKCHAIN SYSTEMS		
Explain blockchain-related regulations, legal aspects, governance, and their impact in the public and private sectors.		
Knowledge	Skills	Responsibility and Autonomy
<b>Knows / Aware of:</b> <ul style="list-style-type: none"> <li>- GDPR requirements and consent management</li> </ul>	<b>Able to:</b> <ul style="list-style-type: none"> <li>- LO2.4: Discuss the interest of Blockchain technology to manage consent and data access</li> </ul>	<b>Capable to:</b> <ul style="list-style-type: none"> <li>- Identify consent management and data usage tracking requirements</li> </ul>
EQF level	EQF Level 5	



## How can you define data protection requirements and GDPR compliance for blockchain systems?

- Are there specific risks regarding personal data?
- What are GDPR key requirements?
- How can you track data usage?
- How can you manage consents?



## How can you define governance and regulation for blockchain systems?

- In this lecture you will
  - Learn GDPR key requirements
  - Learn key principles regarding blockchain compliance with GDPR
  - Learn how blockchain can be used as a support for GDPR implementation, allowing to manage and log consents as well as due usages.

## Learning objectives

### GDPR

Key concepts  
Obligations and rights

### Blockchain regulation constrained by GDPR

Analysis of the blockchain  
context regarding GDPR  
Implementation of GDPR  
key requirements

### Blockchain as a tool for GDPR implementation

Consent management  
Usage tracking

## Table of Content



- ▶ GDPR
  - ❑ Key principles
  - ❑ Obligations and rights
- ▶ GDPR backed blockchain regulation
  - ❑ Blockchain key principles facing GDPR
  - ❑ Implementing key GDPR requirements
- ▶ Blockchain as a GDPR facilitator
  - ❑ Consent management
  - ❑ Data usage tracking
- ▶ To conclude





## General Data Protection Regulation

- EU regulation 2016/679
  - Published in April 2016 and implemented in May 2018
  - Extra-territorial
- Protection scope:
  - Personal data = Data related to a person
    - Identification data
    - Finance
    - Health and genetics
    - Digital life activities and traces
    - Images
    - ...
  - Processes using personal data
    - Manual processes
    - Automated processes
      - Business Processes
      - Statistics and Big Data



## GDPR: key roles

- Subject
  - Person to whom the data relates
  - Must provide an "informed consent"
- Data controller
  - Natural or legal person
  - In charge of designing and controlling the processes using personal data
  - Accountable of the processes
- Data processor
  - Body processing the data on behalf of the data controller
- Data Protection Officer
  - Data security
  - Data protection and usage control



## GDPR: key principles

- Inspired by
  - EU directive 95/46/CE
  - International agreements such as safe harbor or EU-US Privacy Shield
- Fair, lawful and transparent data processing
  - Responsibility of the data controller
  - Data minimisation
    - Collect only the necessary data depending on the purpose
  - Identify clearly usages
  - Purpose limitation
    - Limited to the identified usages
    - Allows data archiving
  - Limited storage
    - Deleting un-necessary data
    - Exception: scientific usage and public interest
  - Checking lawful compliance of data collection
  - Data accuracy
    - Allows subjects to update their data
  - Data integrity and confidentiality

## GDPR: Obligations

- Get subject consent
  - Provide the necessary information given to the subject
    - Understandable
    - Potential usages
    - Information on data processors?
    - Read?
  - Double opt-in
    - Tick a box and confirm
    - Provide a better "proof of consent"
- Data security
  - Risk assessment and implementation of a security policy
  - Communication of data thefts to interested parties within 72 hours
  - Appointment of a Data Security / Protection Officer (DPO)





## GDPR: rights (1)

- Data controllers
  - Transnational data transfer
    - Offset extra-territoriality
  - Co-reponsibility chain including sub-contractors
    - Right or obligation?
  - Legitimate merchant exchanges especially for prospecting (targeted advertising in particular!)
  - Lawful statistic processes
    - If non-discriminatory
    - Without requiring consents for “essential interest” processes
      - Personal life and public health
      - State interest and the fight against tax evasion
      - System Security



## GDPR: rights (2)

- “Living natural persons”
  - Access right for all personal data
    - Explicitly given
    - Automatically collected
  - Informative consent including usages identification, motivation...
  - Right to erasure (reasonable time)
  - Right to be forgotten
  - Simplified right of appeal
    - One authority
    - Passes on demand across the chain
  - Right to get back readable and interoperable data



## Implementing GDPR

- Key principles
  - Appointment of a Data Security / Protection Officer
  - Document data, processes...
  - Adoption of a Privacy by (re)design strategy
    - Privacy impact Assessment
    - Data security policy
    - Highest level of requirement
  - Codes of conduct / labelling
    - Demonstrate compliance
    - Integration of human-related risk management
  - Legal aspect integration
    - Contracts
    - Appeals



## Organising and evaluating GDPR Implementation

- Involvement of
  - Corporate governance
  - Corporate Top management
  - Business departments (HR, marketing, ecommerce...)
  - IT Department
  - Data security / data protection officer
- Implementation evaluation
  - Dedicated surveys associated to the different classes of actors related to
    - Processes
    - Objectives
    - Security processes
    - Legal framework
  - Heavily coupled to the level of cyber hygiene



## Table of Content



- ▶ **GDPR**
  - ❑ Key principles
  - ❑ Obligations and rights
- ▶ **GDPR backed blockchain regulation**
  - ❑ Blockchain key principles facing GDPR
  - ❑ Implementing key GDPR requirements
- ▶ **Blockchain as a GDPR facilitator**
  - ❑ Consent management
  - ❑ Data usage tracking
- ▶ **To conclude**

## Key challenges for GDPR adoption in blockchain systems

### GDPR

- Key GDPR roles
  - Subject
  - Data controllers
  - Data processors
- Process purpose
  - Transparent
  - Fair
- Data access rights
  - Granted to identified subject
  - Data updating
  - Data erasure

### Blockchain

- Immutable and safe block storage
  - Neutral system
  - No change are allowed
- Specific ecosystem
  - Block validators
  - Blockchain developers
  - Users
  - Investors
  - ...
- User Pseudo-Anonymity
  - Key-based identity
  - No link with the real identity





## Redefining basic usages

- Traditional CRUD usages
  - Create / Read / Update / Delete
  - Used for
    - Data access (Read)
    - Data modification (Update)
    - Data erasure (Delete)
- Key blockchain usages
  - CRAB = Create / Retrieve / Append / Burn
  - Used for managing
    - Data access: retrieve
    - Data modification: get the data modify it and add a new record : Retrieve + Append
    - Data Erasure: Burn – Delete the encryption keys of the stored data



## Identity vs anonymity

- Blockchain Users (data subjects or data controllers?)
  - Known as pseudo-identity
    - No link with their real identity?
    - Subject real identification?
  - Subject re-identification
    - Depends on data sources
    - Risk when data sources are mixed
- User activity
  - “Tracked” by the transactions
  - Multiple account tracking?



## Actors role in blockchain vs GDPR

- Blockchain key actors vs GDPR key roles
  - Miners / block validators
    - Do not pay attention to the block content
    - Rather "data processors"
  - Developers
    - Provide the technical means for data processing
    - Are not aware of the data usage
  - Blockchain service layer / application layer members
    - Manage different kinds of data
    - May be data controllers
  - Blockchain investors
    - May identify different usages
  - Blockchain users
    - Blockchain as a part of an Information system => Data controller
    - End-users => Subjects or data controllers?

## Data controller key role identification

- Usage accountability
- Private and permissioned blockchains
  - Clear identification of the usages and roles
  - Well identified consortium
  - Clear identification of the data controllers
- Public blockchain
  - Collective processing
  - No clear responsibility
    - BUT blockchain may be considered as a part of a global process
    - End users are also responsible for deciding which information is stored in the blockchain
  - Still under debate...





## Blockchain vs GDPR key rights

- Blockchain stores blocks:
  - In a distributed way
    - Increase data availability
    - May increase security risks
    - Extra-territoriality => No real control about data transfer
  - Consistently and safely
    - Transparency
    - Data extraction fits data portability right
    - Data can be accessed => fits the right to access data about you
  - Immutably
    - Data cannot be modified / deleted, except when append and burn services are set
    - No right to be forgotten
- Requires
  - Identification of the data controller
  - Data constraints:
    - Anonymised data
    - "Immutable" / public interest data
    - Data encryption coupled with key destruction => Erasure?

## To conclude on GDPR implementation in blockchain system

- Blockchain technology
  - Still immature
  - Technical tool among others
- Usages
  - Clearly identified
    - Minimisation of the necessary data set
    - Integration in a complete process
  - Data protection
    - Encrypted / obfuscated data stored in the blockchain
    - Difficult to detect intrusion in a distributed ledger



## Table of Content



- ▶ GDPR
  - ❑ Key principles
  - ❑ Obligations and rights
- ▶ GDPR backed blockchain regulation
  - ❑ Blockchain key principles facing GDPR
  - ❑ Implementing key GDPR requirements
- ▶ Blockchain as a GDPR facilitator
  - ❑ Consent management
  - ❑ Data usage tracking
- ▶ To conclude



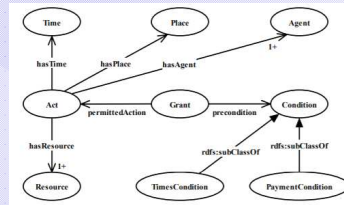
## Consent management

- Obligation of the data controller:
  - User must be aware and must consent
    - to the data collection
    - to the data processing
  - Processes must be done according to the user consent
- Key questions:
  - Proving that the consent has been given
  - Proving that the process fits the allowed usages
- Requires
  - Immutable storage of consents
  - Logs of usages



## Using a blockchain to manage consents – Defining consent model

- Consent similar to access right?
  - Subject
  - Object
  - Usage
  - Decision (allow / deny)
  - Conditions including time validity



OREL ontology model picked from Qu, Yuzhong, Xiang Zhang, and Huiying Li. "OREL: an ontology-based rights expression language." Proceedings of the 13th international World Wide Web conference on Alternate track papers & posters. ACM, 2004

## A purpose-based usage model

- Process purpose
  - Usage operations
    - Extend the CRUD operations
    - Manage data replication and exchange
  - Organizational context
    - Identify the exact goal depending on the process chain organisation
    - Allow defining the subject of the access right
  - Business context context
    - Process purpose
    - Business scope
    - Process motivation



## Blockchain-based consent storage

- How to prove a consent?
  - Store a time-stamped encrypted version of the consent
  - Allow consent evolution by creating new time-stamped consents
- Data retrieval function
  - Extract consent AND time-stamps
  - Proof for
    - Subjects
    - Data controllers
- What is stored in the blockchain
  - The encrypted consent
  - A hash of the consent



## Proving data usage thanks to blockchain

- Using smart contract to implement access control function
  - Allow user retrieve the exact smart contract
  - Define precise usage rules and conditions
  - Smart contract can transfer the access token to the requester
  - Associated risks:
    - Smart contract activation condition
    - Grant access token to unauthorized account
- Using smart contract to transfer data encryption key to the data processor
  - Depending on usage condition
  - Encrypted data are stored separately
  - Data “consumer” gets the key to decrypt the requested data
    - Key associated to the data is encrypted so only the right data consumer can get access to it





## Blockchain as a GDPR support

- Different application services
  - Personal Information Management systems
  - Consent management
  - Access control
- Based on permissioned blockchain
  - Ensure limited access
- Minimising personal data
  - Only access rights are stored
    - For consents
    - For authorising accesses

## Table of Content



- GDPR
  - Key principles
  - Obligations and rights
- GDPR backed blockchain regulation
  - Blockchain key principles facing GDPR
  - Implementing key GDPR requirements
- Blockchain as a GDPR facilitator
  - Consent management
  - Data usage tracking
- To conclude



## To conclude

- **GDPR**
  - A legal framework for manipulating data
    - Rights and duties of service providers
    - Constraints to prove good faith
  - Limited by the practices of the users themselves
    - No experience on extra-territoriality
    - Inconsistent data exchange
  - How to find the "root cause" of the disclosure of personal data
    - Issue for Service Providers
    - How to prove that the leak does not come from them
    - How to identify an intrusion quickly: average time to detection 240 days!
- Extra requirements in the new Data Governance Act



## To conclude

- **Blockchain vs GDPR**
  - Hard to identify GDPR key actors
    - Data controllers
    - Subjects
  - CRAB vs CRUD operation
    - Data erasure
    - Data modification
  - Blockchain can be a support for GDPR
    - Storing consents
    - Managing accesses thanks to smart contracts





## Resources

- <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
- [https://www.europarl.europa.eu/stoa/en/document/EPRS\\_ATA\(2018\)624254](https://www.europarl.europa.eu/stoa/en/document/EPRS_ATA(2018)624254)
- <https://www.eublockchainforum.eu/reports/blockchain-and-gdpr>
- <https://iapp.org/resources/article/blockchain-and-gdpr/>
- Humbeek, A. V. (2019). The blockchain-GDPR paradox. *Journal of Data Protection & Privacy*.
- Data Governance act: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52020P00757>
- Haque, A. B., Islam, A. N., Hyrynsalmi, S., Naqvi, B., & Smolander, K. (2021). GDPR compliant blockchains—a systematic literature review. *IEEE Access*, 9, 50593-50606.
- Truong, N. B., Sun, K., Lee, G. M., & Guo, Y. (2019). Gdpr-compliant personal data management: A blockchain-based solution. *IEEE Transactions on Information Forensics and Security*, 15, 1746-1761.
- Berberich, M., & Steiner, M. (2016). Blockchain technology and the GDPR-how to reconcile privacy and distributed ledgers. *Eur. Data Prot. L. Rev.*, 2, 422.



## Get In Touch

### Social Media

@ CHAISE.EU

### Website

chaise-blockchainskills.eu

### Email

