SOTER

Training Handbook: **BLOCKCHAIN**

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833923

Authors: José Manuel Panizo Plaza and Robin Renwick
Design and Layout: Matthew Reilly and Ekaterina Kyulyumova

Published in January 2022 (Graz/Dublin/Madrid)

ISBN: 978-3-903374-12-6
DOI: 10.25364/978-3-903374-12-6

Table of contents

SOTER Training Handbooks Introduction

The financial sector is experiencing a real digital revolution in recent years, in which traditional entities are becoming providers of digital services in order to remain competitive. Although it is clear that this new era implies many advantages for businesses and citizens, in addition, the release of new digital services and connections imply the appearance of new threats and risks in terms of cybersecurity, data privacy and the use of digital identities.

These threats must be tackled under a holistic approach and pointing at their different origins, including the human factor.

Furthermore, the current regulations to be met, apart from involving a technological and mind-set challenge and increasing the number of entities with which to interact with, also aim to create or improve tools to prevent fraud and reduce cyber vulnerabilities as much as possible.

SOTER takes the challenge, considering both technological and non-technological (human factor and governance within organizations) aspects and providing innovative solutions that will act as a transformative process of the finance sector, helping their players to increase their cybersecurity level, improving the fight against present and future cyber attacks and vulnerabilities and, to summarise, increasing their cyber-resilience.

SOTER tackles two main challenges: how to improve the process of digital onboarding and how to implement state of the art cybersecurity culture.

This handbook summarizes the outcomes on the SOTER work on blockchain

1

Blockchain in SOTER

Blockchain technology is a type of data structure built on state of the art cryptography. The technology is used in SOTER to allow banking clients a way of storing and sharing their digital identity credentials, when they require. It also provides a secure way for finance service providers to verify the identity of new customers – safe in the knowledge that the identity presented to them has not been tampered with.

1.1. Introduction to Blockchain

The concept of a blockchain falls under a wider term which is called "Distributed Ledger Technologies", or DLT. This refers to the new paradigm in sharing and storing information. As the name suggest, it implies the existence of a:

- Distributed database: Data is not kept as a single copy, but rather it is stored distributed between nodes of a network. It can be seen as a database located in multiple places and being processed as a single unit. A distributed system should be consistent – each node has the same information at a certain point of time- and be failure tolerant, meaning that if one node fails to operate correctly this does not impact the correct functioning of the network as a whole.
- Ledger: The information is presented through a record of transactions between accounts or users of the infrastructure. These transactions can refer to the transfer of assets or to the change in the status of some piece of information, registered, shared, synchronized, and verified by the nodes of the network. The above permits data to be stored resiliently, since it is kept by several nodes in a verifiable and transparent manner, due to the availability of the information. A DLT may or may not be decentralized. Decentralization implies that the need for verification or approval by a central authority is removed, with responsibilities shared between different actors within the network. With such a property, data is filed independently from the validation of a trusted third party. The endorsement of the information is obtained through a consensus mechanism between some, or all, of the involved agents.

A blockchain is a type of DLT. It contains information in records, stored in blocks. The blocks are linked in a list using cryptographic techniques. Each block has some meta-information, such as a timestamp and the hash of the data contained in the previous block. When a block is appended to the chain, all the nodes of the network must reach agreement. If the block is confirmed, all the nodes must process it along with the included transactions. Although the most known use of blockchain technologies relates to cryptocurrencies, transactions should not be seen as only financial operations. A transaction is a just a change in the state of an item. Blockchain technologies offers appealing characteristics such as:

- Immutability: Once data is stored in a block, and the block is confirmed by the network, the information cannot be altered without rebuilding the remaining chain. This is a layer of security which ensures that data, once appended to the chain, cannot be altered by any one party without substantial effort and significant resources. Any change in previously confirmed data must be confirmed, and accepted, by other members in the network through the protocol consensus mechanism.
- Transparency: Transactions and changes of state of data are shared between all the organizations that have permission to view the stored information. This adds a degree of accountability to the data store, which is extremely beneficial for the financial industry, as state changes are recorded accurately, and consistently, according to the protocol rules of the network.
- Trustless: Participants in the network agree to run a consensus protocol, used to reach agreement on new state changes and/or transactions. There is no one source of truth for the network, as the order of events is agreed upon by all parties in a synchronous manner.

In this way, a decentralized ledger is a trustless system as there is no need to delegate trust to a third-party for an agreed order of events within the network.

1.2. Taxonomy of blockchains

In this section, a taxonomy will be established to classify the different blockchain implementations that are available currently. It will be considered who is granted read and write access permission to the information stored in the blockchain.

Data Access: Public and Private blockchains

From the point of view of establishing access and modification to the stored information, a blockchain can be defined as public or private. In a public blockchain, there are no restrictions on reading data or on who can propose transactions to be included by the network (append/modify data). It is generally riskier, as anyone can take part in the blockchain mechanism, as long as they partake according to the consensus ruleset. In a private blockchain read access and append/modify access is limited to a closed group of nodes, which are controlled by a regulator or private consortium. The nodes in the network all agree to partake according to the consensus ruleset.

Network Access: Permissioned and Permissionless blockchains

Taking into account the perspective of which nodes can process transactions, other classification can be established. In a permissionless blockchain, the capacity of joining the network is offered to any prospective node. There are no rules for joining the network and for becoming involved in the processing of transactions. By contrast, in a permissioned blockchain, only a close list of identified and vetted nodes are able to join the network and process transactions. This divergence is related to the governance of the blockchain.

1.3. Use in the finance sector

Onboarding and KYC/Identity

In the finance sector there is a legal requirement for service providers to know who their customers are. This is to maintain security and stability of the sector as a whole, and also to assist law enforcement agencies when there is a request for information regarding the finance activity of a person. Know Your Customer (KYC) processes are a critical element of service providers overall risk management and customer due diligence processes.

The KYC process is an identity verification process. The client provides a set of attestations, credentials, or proofs – that state who they are, where they are from, their nationality, their address, their physical features, etc. The most well-known is a passport – which provides a number of data points related to the person presenting them. This information is verified against other data points, like a national ID card, a driver's licence, a birth certificate, as well as other data points such as a video recording, a digital photo, or even a fingerprint scan.

All the information gathered about the person helps to verify the person is who they say thy are – with the goal of reducing fraud and preventing identity theft. This is becoming more important in the 21st century when so much of our activity is moving online.

DIDs, VCs, and Identity Wallets

Society is demanding a new paradigm of Digital Identity, focused on users, more secure and legally. In recent years the self-sovereign model has emerged to fullfill new demands. In this model, the digital identity of a user will inform an entity about his or her identity attributes, which are discrete pieces of information linked to a specific user. It should be built upon a decentralized identity

paradigm, which can be achieved shifting most of thecapabilities to a user's hands, or at least trusting in decentralized methods and cryptographic algorithms. This identity system should provide end-users a digital sovereign identity, where the user will be the absolute owner of his or her personal data. He or she will manage the access to the information along with the possibility of sharing it. In The path to Self-Sovereign Identity, Allen defined ten principles of Self-Sovereign Identity:

- Existence - People have an independent existence.
- Control - People must control their identities.
- Access - People must have access to their own data.
- Transparency - Systems and algorithms must be open and transparent.
- Persistence - Identities must be long-lived.
- Portability - Information and services about identity must be transportable.
- Interoperability - Identities should be as widely usable as possible.
- Consent - People must freely agree to how their identity.
- Minimization - Disclosure of claims must be minimized.
- Protection - The rights of individual people must be protected

The community has described a framework to interchange personal data attributes in a privacy and user-centric manner. The key piece of this is the Verifiable Credential. A credential can represent all the information that a physical credential represents. It might be information related to identifying its subject (a name or an identification number), to the issuing authority (a government or a certification body), to information about the type of credential (a driving license) or to specific attributes being asserted by the issuing authority about the subject (the classes of vehicle entitled to drive). Some cryptographic techniques, such as digital signatures, are added to credentials to make them verifiable which ensure the credential is tamperevident and trustworthy.

Verifiable Credentials management involves these actors:

- Holder: A entity that possesses one or more verifiable credentials and can generate verifiable presentations from them.
- Issuer: A entity that asserts information (claims) about subjects, and creates verifiable credentials from these claims and sends them to a holder.

- Subject: an entity (end-user or organization) about which claims are made. The role of the holder usually is the same than the subject, but it in some cases a holder can keep the credential of a subject (for example, a parent and a child).
- Verifier: An entity who receives, verifies and processes credentials

The entities involved in verifiable credentials are represented and identified by decentralized identifiers (DIDs). A DID is an identifier which points to a DID Document, a data structure. This piece of information contains one or more service endpoints for interacting with the entity identified by the DID, and also public keys to enable entities authentication. Following Privacy by Design principles, one entity can create as many DIDs as it needs to establish a secure separation of contexts. DIDs can be created, read, updated or deactivated in a specific blockchain. Thanks to the identity management provided by DIDs, the dependence on centralized registries or hierarchical PKI is eliminated. Using the advantages of blockchain technologies, DIDs framework provides the following benefits:

- Decentralization: Eliminate the requirement for centralized authorities or single point failure in identifier management, including the registration of globally unique identifiers, public verification keys, service endpoints, and other metadata.
- Control: Give entities, both human and non-human, the power to directly control their digital identifiers without the need to rely on external authorities.
- Privacy: Enable entities to control the privacy of their information, including minimal, selective, and progressive disclosure of attributes or other data.
- Security: Enable sufficient security for relying parties to depend on DID documents for their required level of assurance.
- Proof-based: Enable DID subjects to provide cryptographic proof when interacting with other entities.
- Discoverability: Make it possible for entities to discover DIDs for other entities to learn more about or interact with those entities.
- Interoperability: Use interoperable standards so DID infrastructure can make use of existing tools and software libraries designed for interoperability.
- Portability: Be system and network-independent and enable entities to use their digital identifiers with any system that supports DIDs and DID methods.
- Simplicity: Favour a reduced set of simple features to make the technology easier to understand, implement, and deploy.
- Extensibility: Where possible, enable extensibility provided it does not greatly hinder interoperability, portability, or simplicity

Users can protect all theirverifiable credentials together with the private keys associated with the DID-public keys in a secure storage called wallet. This vault can be an application in a smartphone, or a cloud service, and must be under the solely control of its owner. A wallet must provide interfaces to request and storage credentials, but also to deliver and present them. Wallets also offer authentication capabilities, signing challenges to show that its owner possesses the private key associated with a DID.

1.4. Role of blockchain in this

An instance of blockchain offers a distributed and decentralized repository of information together with its well-known advantages such as tamper-evidence, censorship resistance and transparency. Therefore, the ledger constitutes a trust third-party to anchor the link between the DID and the public key that verifies its control.

2

Threats and Risks

This section addresses the threat and risk spectrum tackled by the SOTER project

Ledger security

Cryptographic security

Wallet security

One of the most common attacks in blockchain is the 51% attack. In this case, several notable cryptocurrencies such as ZenCash, Monacoin, Bitcoin Gold Verge and Ethereum Classic were victims of 51% attacks in 2018. Ethereum Classic was impacted by a 51% attack in 2020.

Another important attack to consider in blockchain is the denial-of-service attack. Attackers can perform this type of attack against honest nodes, ignoring any messages that the attackers do not generate. The attack vector for executing these attacks in blockchain is through the consensus mechanism. By controlling the majority of consensus nodes, attackers can control the aggregated content. An example of such an attack occurred in the summer of 2017 where a DDOS attack targeted the Bitcoin cryptocurrency system, resulting in a performance slowdown.

3

Risk Mitigation

As blockchain based identity services are currently not deployed on the market, we focus here on a compact discussion of mitigation options for risks involved in this technology.

Governance

The organisational model of the blockchain network is as important as the underlying technology, so a governance framework should be established to create guidelines and procedures which define:

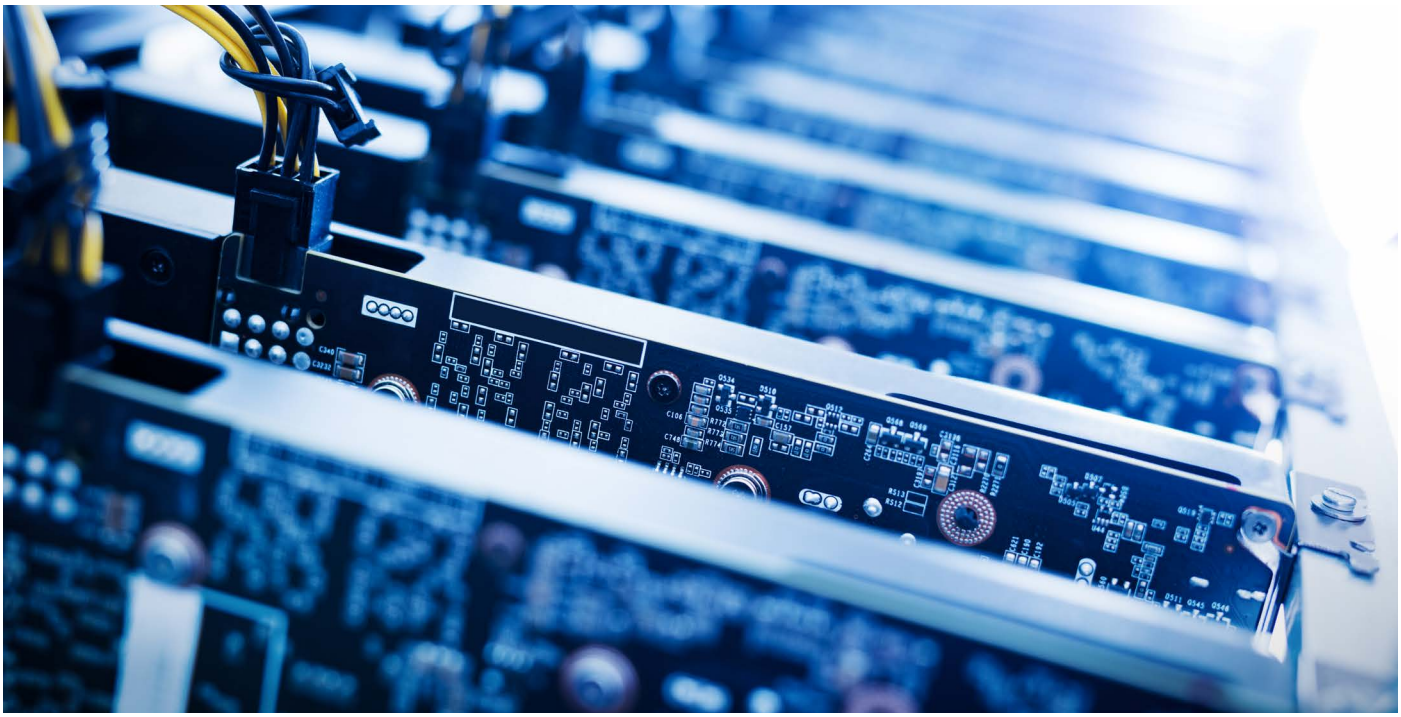
- Who is granted read and write access permission to the information stored in the blockchain.
- How participants in the blockchain reach consensus on any proposed appending of data.
- How members are identified, and how their credentials are managed and/or appraised.
- Within the scope of GDPR, what is the role of each member.

Regarding the rights that a node neds to participate in a blockchain, the governance body must determine the identification and authentication policies, depending of the type of blockchain developed. These policies should include:

- The list of entities which take part in the blockchain network (through the possession of a node), and how they will be identified.
- A secure storage mechanism where the set of authorized identities will be kept.
- The correct access levels that the entities own.
- The on-boarding mechanism to add a new member to the blockchain network.
- Furthermore, a crucial aspect is the management of the credentials that the entities will use to authenticate the participant nodes in the blockchain network. These credentials should maintain a secure life cycle, and the processes for issuance, renewal, verification and revocation should be considered. Finally, the responsibilities of participants should be communicated through some form of contract when these credentials are activated.

4

Compliance and Regulation



4.1. GDPR

The General Data Protection Regulation (GDPR) is a legislative instrument that came into force in 2018. It applies to the processing of personal data, defined in Art 4 (1) GDPR as "any information relating to an identified or identifiable natural person". An identifiable natural person is "one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".[1]

The individual claims processed using blockchain technology are personal data according to Art 4 (1) GDPR, if they relate to an identifiable natural person. The natural person is identifiable due to specific data points collected and processed, such as: name, phone number, date and place of birth, photo, biometric face template, etc. Pseudonymisation of this data does not eliminate the relation of the data to the identifiable individual, because a person is still deemed identifiable even if additional information is required in order to connect the data processed on the blockchain to a specific individual.[2]

GDPR obliges processors of personal data act according to certain rules, ensure data is processing according to a lawful basis, whilst maintaining consideration of key data protection principles. The GDPR also mandates that individuals are able to exercise the data protection rights bestowed onto them by the legislative act.

The processing of personal data is defined in Art 4 (2) GDPR as "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording,

1 [European Parliament and of the Council. (2016). Art. 4 (1) GDPR – Definitions | General Data Protection Regulation (GDPR). European Parliament and of the Council. https://gdpr-info. eu/art-4-gdpr/

2 Anderl/Schelling, Datenschutzrechtliche Grundlagen in Anderl (Hg), Blockchain in der Rechtspraxis (2020) 91.

organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction".[3]

As Verifiable Credentials are personal data, they should not be stored directly on blockchain. Therefore, it is necessary to apply pseudonymisation. Pseudonymisation consists of replacing personal data by other information, which does not directly allow the identification of a natural person. The selected method to store credentials in the blockchain is hashing. This process is conducted to reduce linkability concerns. In the SOTER solution, two hashes are produced.

- Attestation hash: pseudonymised identifier is created by hashing the verifiable credential along with a random variable and an issue code. It is used to register that a credential has been issued. It is a mechanism to guarantee the integrity of the original credential and allows relying parties to verify the issuance of a credential by a trusted party.
- Revocation hash: once the credential is issued and delivered to the user wallet, the revocation hash is also calculated. Whenever a credential is no longer valid, the revocation hash can be registered on the blockchain. At any time, a relying party can check if a revocation hash exists on the blockchain. This allows a party to verify that a credential is valid, as if the revocation hash is not present, they can assume the credential is valid.

Blockchain technology can be implemented in ways that promote transparent, auditable, and secure processing of data. However, consideration must be given to what data is appended to the ledger, and by whom, who has access to the data, and what governance mechanisms are in place to ensure correct distribution of both responsibility and liability.

4.2. PSD2

The second Payment Services Directive (PSD2) progressively came into force in Europe between 2018 and 2019. It governs electronic payments across Europe and was an update to the original Payment Services Directive enacted in 2007. PSD2 updated the legislation and seeks to boost competition, consumer protection, and innovation in the European payment services market.

The European Commission has outlined the key points of PSD2 as follows:

The directive seeks to improve existing EU rules for electronic payments. It considers emerging and innovative payment services, such as internet and mobile payments.

The directive sets out rules concerning:

- Strict security requirements for electronic payments and the protection of consumers' financial data, guaranteeing safe authentication and reducing the risk of fraud;
- The transparency of conditions and information requirements for payment services;
- The rights and obligations of users and providers of payment services.[4]

PSD2 included some major updates, most notably concerning how third-party service providers (TPPs) access the sector. This included the definition of two concepts – Payment Initiation Services (PISP) and Account Information Providers (AIP).

3 European Parliament and of the Council. (2016). Art. 4 (2). https://gdpr-info.eu/art-4-gdpr/

4 Revised rules for payment services in the EU, a summary from the European Commission on PSD2, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:2404020302_1

PSD2 outlines the roles and obligations of parties involved in the payment services industry, with the goal of increasing security and consumer protection, as well as providing a market that fosters innovation, and maintains crucial data protection rights.[5]

One of the core security focused updates to the Directive was the inclusion of obligations and rules concerning Strong Customer Authentication (SCA), which outlines the methods and procedures required to ensure the provision of secure payment services across Europe. The mandate to require Strong Customer Authentication has bolstered the security of online financial transactions across Europe and ensured that customer identification and authentication are at the centre of a robust electronics payments sector.

4.3. eIDAS2

The electronic identity and trust services (eIDAS) regulation is a European regulatory framework that attempts to create European-wide harmonisation for the provision of identity and trust services across Member States. The regulation's intention is:

> "...to enhance trust in electronic transactions in the internal market by providing a common foundation for secure electronic interaction between citizens, businesses and public authorities, thereby increasing the effectiveness of public and private online services, electronic business and electronic commerce in the Union."[6]

eIDAS provides a set of guidelines for the identification of individuals and associated infrastructure to ensure that digital or electronic identification processes are harmonised across Member States. The regulation also governs the provision of Trust Services (TS) – such as electronic signatures, notarisation, and timestamping – critical components for a European wide online transaction architecture that is both secure and trustworthy.

eIDAS is currently being amended, with a revised eIDAS2 currently in consultation.[7] The revision outlines specific rules and obligations for European wide digital identity, with special focus on the obligations of Member States to provide a service that is interoperable and compatible across Europe.

The revised regulation also widens the scope to include the private sector, and allows European states to nominate a digital identity service provider to operate the State's identity service. Crucially, the regulation also promotes the concept of Self-sovereign Identity (SSI), as part of the ongoing European Self-sovereign Identity Framework (ESSIF) lab initiative which seeks provide the foundations for a "next generation, open and trusted digital identity solution for faster and safer electronic transactions via the Internet and in real life".[8]

5 Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR, Version 2.0, Adopted on 15 December 2020, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202006_psd2_afterpublicconsultation_en.pdf

6 Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, Available at: http://data.europa.eu/eli/reg/2014/910/oj, (2).

7 EU digital ID scheme for online transactions across Europe, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12528-EU-digital-ID-scheme-for-online-transactions-across-Europe_en

8 https://essif-lab.eu/

4.4. AML6D

The finance sector is a highly regulated industry, with a host of applicable legislative instruments governing how entities engage in the market for financial related products and services. One of the central legislative pillars of the sector is the 5th Anti Money Laundering Directive (AML5D), currently in force across Europe.

AML5D is a wide-ranging directive, that mandates finance sector entities maintain appropriate controls to counter the threat of money-laundering and terrorist financing. The regulation impacts the required processes concerning the identification of the data subject, the verification of that entity by a trusted entity, and the evidential framework required to be put into place regarding Know Your Customer (KYC) and Customer Due Diligence (CDD) processes.

AML5D, like eIDAS, is also in an amendment cycle - with the proposed Anti-Money Laundering (AML6D) package currently in consultation phase.[9] AML6D seeks to further harmonise existing legislation, provide improved clarity concerning both private sector and Member State obligations, includes the regulation of financial instruments such as cryptocurrency and crypto-assets, increases the obligations regarding traceability and linkability, and creates a dedicated AML regulatory body (Anti-Money Laundering Authority) to oversee the implementation of the revised legislative package.

References

[1] European Parliament and of the Council. (2016). Art. 4 (1) GDPR – Definitions | General Data Protection Regulation (GDPR). European Parliament and of the Council. https://gdpr-info.eu/art-4-gdpr/

[2] Anderl/Schelling, Datenschutzrechtliche Grundlagen in Anderl (Hg), Blockchain in der Rechtspraxis (2020) 91.

[3] European Parliament and of the Council. (2016). *Art. 2 (1) GDPR – Definitions | General Data Protection Regulation (GDPR)*. European Parliament and of the Council. https://gdpr-info.eu/art-2-gdpr/

[4] Ibid, Art. 4 (2) GDPR

[5] European Parliament and of the Council. (2016). Art. 4 (6) GDPR – Definitions | General Data Protection Regulation (GDPR). European Parliament and of the Council. https://gdpr-info.eu/art-4-gdpr/

[6] Stadler/Bichler, Die Blockchain-Technologie im Lichte der DSGVO, ZIIR 2019, 382 (383).

[7] Paal/Pauly, Art 2 DS-GVO Rz 6, beck-online.

[8] European Union. (2016). Recital 26 - Not Applicable to Anonymous Data | General Data Protection Regulation (GDPR). https://gdpr-info.eu/recitals/no-26/

[9] Ibid, Recital 28

9 nti-money laundering and countering the financing of terrorism legislative package, https://ec.europa.eu/info/publications/210720-anti-money-laundering-countering-financing-terrorism_en