Master's thesis

Master's Programme in Computer Science

GDPR, Blockchain and the Right to be Forgotten

Tsegaye Ture

September 7, 2021

Faculty of Science

University of Helsinki

Supervisor(s)

Prof. Valtteri Niemi

Examiner(s)

Contact information

P. O. Box 68 (Pietari Kalmin katu 5)
00014 University of Helsinki,Finland

Email address: info@cs.helsinki.fi
URL: http://www.cs.helsinki.fi/

HELSINGIN YLIOPISTO – HELSINGFORS UNIVERSITET – UNIVERSITY OF HELSINKI

Tiedekunta — Fakultet — Faculty	Koulutusohjelma — Utbildningsprogram — Study programme
Faculty of Science	Master's Programme in Computer Science

Tekijä — Författare — Author

Tsegaye Ture

Työn nimi — Arbetets titel — Title

GDPR, Blockchain and the Right to be Forgotten

Ohjaajat — Handledare — Supervisors

Prof. Valtteri Niemi

Työn laji — Arbetets art — Level	Aika — Datum — Month and year	Sivumäärä — Sidoantal — Number of pages
Master's thesis	September 7, 2021	68 pages

Tiivistelmä — Referat — Abstract

The introductory section of the thesis discusses on the European General Data Protection Regulation, abbreviated GDPR, background information and historical facts. The second section covers basic concepts of personal data and GDPR enforcement. The third section gives detailed analysis on data subject rights as well as best practices for GDPR compliance to avoid penalties. The fourth section concentrates on the technical aspects of the right to be forgotten, solely concentrating on the technical aspects of permanent erasure/deletion of personal or corporate data in compliance with the customer's desire. Permanent deletion or erasure of data, technically addressing the issue of the right to be forgotten and block chain network technology are the main focus areas of the thesis. The fifth section of the thesis profoundly elaborates block chain and the relation with GDPR compliance in particular. Then the thesis resumes explaining about security aspects and encryption, confidentiality, integrity and availability of data as well as authentication, authorization and auditing mechanisms in relation to the GDPR. The last section of the thesis is the conclusion and recommendation section which briefly summarizes the entire discussion and tries to suggest further improvements in future works to be done thereby recapitulating the main points raised in the thesis overall.

ACM Computing Classification System (CCS)
Security and privacy → Human and societal aspects of security and privacy → privacy protections
Applied computing → Law, social and behavioural sciences → Law

Avainsanat — Nyckelord — Keywords

GDPR, block chain, privacy

Säilytyspaikka — Förvaringsställe — Where deposited

Helsinki University Library

Muita tietoja — övriga uppgifter — Additional information

Networking study track

Contents

1 Introduction

In January 2012, the European Commission presented the draft of a new *General Data Protection Regulation (GDPR)* to the European Parliament and the Council of the European Union. After the draft were presented to the EU parliament and council, rigorous preparation and debate was undertaken among the stakeholders before the GDPR was eventually accepted and approved unanimously and unequivocally by the EU parliament on 14 April 2016 in Brussels, see Figure 1. The new data privacy and protection legislation was implemented on 25 May 2018.

The intentions behind the new GDPR are commendable. The main purpose of the GDPR is to protect the fundamental rights and freedoms of individuals, in particular their rights to protection of personal data. The GDPR applies in a society where commercial enterprises and authorities have rapidly increasing capabilities to collect, store and combine personal information. The GDPR facilitates free movement of personal data within the European Union through a uniform legislation in all member states.[Nyrén et al., 2014]

The GDPR comprises two categories of regulations. The first category applies to any type of personal data processing. The second category involves particular rules that apply to processing of special types of personal data that are sensitive in nature, such as health data. Health data is critical for scientific research, including clinical and transnational research sectors. Therefore scrupulous consideration of the new rules is very important while conducting scientific researches and processing sensitive personal data.

In general, sensitive data is any data that reveals one of the following: racial or ethnic origin, political opinion, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data, sex life or sexual orientation, financial information (bank account numbers and credit card numbers) as well as classified information.

The utilization and processing of these special categories of data is strictly regulated and researchers need to adapt the procedures articulated in GDPR guidelines while practicing scientific project findings and ensure compliance to the GDPR enforced in May 2018. Otherwise violation of the regulation, no matter what vital findings are obtained in conducting the research, will have penal repercussions. [Nyrén et al., 2014]

The European General Data Protection Regulation is a profound change in the history of

data privacy and protection. All companies legally operating in the territories of European Union countries are expected to comply with it. The regulation also applies to companies running their business beyond EU extraterritorial borders while functionally operating on data collected from EU countries. The law obliges these companies to conform to the procedures without any dispensation and be vigilant with personal and corporate data governance while doing business in EU member countries. Companies need to handle data privacy meticulously. [Kuner, 2012]

Data subjects in the GDPR context or literally all individuals have the right to know what kind of data has been collected about them and how the handling party is making use of their data. The regulation also obliges companies, upon request, to stop using personal data or to hand it over to the individual. Companies not complying and unwilling to cease using personal data upon request encounters tiered hierarchical fines based on the severity of the violation. [Purtova, 2018]

Business operations became significantly complicated for companies that process any kind of personal data of European Union residents after the introduction and acquisition of the GDPR. By the end of 2018, 50% of companies affected by GDPR were not in full compliance with its requirements. One of the requirements for companies to fulfil compliance with GDPR is to implement sophisticated technologies for protecting data ownership. These technologies should detect violations against copyrights in compliance with the relevant GDPR article. The technologies should also block the violations from appearing online. Companies should have effective content recognition systems that automatically detect problematic content that is against community guideline standards and remove it from the Web. [Politou et al., 2018]

Figure 1.1: European Union Parliament
[Source from European Parliament Portal]

2 Basic concepts of GDPR

The GDPR replaced the 1995 Directive 95/46/EC, which constituted the former European legal framework for processing of personal data. The new GDPR 2016/679 of 27 April 2016 on the protection of data subject rights regarding the processing and utilization of personal data and on the free movement of data as a freedom of expression, renouncing Directive 95/46/EC, boosts and correlates the rules for protecting data subjects' privacy rights and freedoms within and, under certain conditions, outside the EU territory.[Nyrén et al., 2014]

The new regulation concentrates on personal data privacy and protection in which some depict it as a hindrance to smooth business operation and a setback to medical research accomplishment. The regulation, however, merely requires compliance and companies to request for permissions from the data subject, owner of the data before distributing or leaking sensitive information. This may have severe ramifications and might cause impediments for smooth business operations and medical researches if leaked without permission. Dissemination of delicate and confidential personal information such as medical history, credit card details, biometric data etc. causes impending psychological, social, political, technological and economic financial damages if the information falls to the hands of unauthorized entities or personnel.[Nyrén et al., 2014]

The GDPR makes it clear that individual people known as data subjects are the owners of their personal data. The GDPR gives special emphasis to 'personal data', meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. These personal identifiers include name, social security number SSN or identification number, geographical data or unique online identifier.[Nyrén et al., 2014]

To alleviate issues associated with GDPR awareness, compliance and enforcement implementation, the EU commission aspires to reinforce the role of data protection authorities by inspiring member states to grant adequate resources to them, as well as boost collaboration among them. The EU's executive body also intends to ensure data regulators apply GDPR in a constant manner so that the enforcement is applied uniformly and consistently across the 28 countries. The EU commission cautions that the success of the regulation should not be measured by amount and number of fines inflicted, but by transformations

in the culture and behavior of all actors involved. Rather than striking tremendous data collecting companies like Google, FaceBook, Mariott, British Airways and others with multi-million-Euro fines, data protection officers have other better alternatives at their disposal such as imposing a provisional or unconditional restriction on data processing, including a sanction, or instructing the interruption of data flows to a recipient in a third country. [Voss, 2017]

In some cases, the investments required for getting an institution just to comply with the new GDPR rules could cost ridiculously large sum of money which includes hiring experts on data protection and privacy. If spent wisely, however, the compliance costs could be converted into business investments without additional expenses.[Burri and Schär, 2016]

2.1 GDPR enforcement

This new and historic GDPR legal milestone both prolongs and updates the EU acquisition of the former Data Protection Directive 95/46/EC. Before the advent of the newly enforced GDPR, the former data protection rules across Europe were first introduced during the 1990s and had staggered to cope up with rapid technological changes. The directive was implemented on 5 May 2016 and EU countries adopted it into their national law by 6 May 2018. The directive guarantees the protection of fundamental rights of a natural person even whenever their data is accessed by criminal law enforcement officers for law enforcement purposes. This will particularly ascertain that the personal data of victims, witnesses, and suspects of crime are appropriately protected and will enable cross-border cooperation in the fight against crime and terrorism. [Burri and Schär, 2016]

After the GDPR was published in the EU Official Journal for the first time in May 2016, it was enforced in May 25, 2018. The two years rigorous deliberation period has given private businesses and public administrations sufficient time to prepare for the fundamental changes introduced by the regulation. There have been enormous amount of data breaches such as details of accounts on LinkedIn, Yahoo, MyDpace etc in recent times which affected data subjects confidential information such as passwords, residential address and credit card details. [Burri and Schär, 2016]

The information commission officer of the GDPR should briefed about any breach within 72 hours after an organization discovers the incidence and the impact on the victims of the breach should be assessed. Any unauthorized divulgence, access, alteration and destruction of people's data might have detrimental ramifications and must be reported

to the country's data protection regulator. For companies hiring more than 250 employees, documentation of the motive for collecting and processing of people's data, the description of the recorded information and the duration it is going to held as well as the technical security measures implemented should be revealed. [Voss, 2017]

Data protection officer is an important role required by the GDPR for large businesses, public authorities or companies that regularly monitor and conduct massive scale processing of individual's data or sensitive information. The person in this role or position has to report to senior staff members, ensure GDPR compliance as well as serve as a point of contact for employees and customers. The GDPR enforced in May 2018 is an evolution not a revolution. [Nyrén et al., 2014]

The Reform consists of two instruments :

The General Data Protection Regulation

The GDPR will enable people to better control their personal data. At the same time modernized and unified rules will allow businesses to make the most of the opportunities of the digital single market by cutting red tape(bureaucracy, excessively complicated administrative procedure)and benefiting from reinforced consumer trust.[Wachter et al., 2017]

The Data Protection Directive

This directive is intended for the police and criminal justice sector. The directive guarantees the protection of fundamental rights of a natural person even whenever their data is accessed by criminal law enforcement officers for law enforcement purposes. This will particularly ascertain that the personal data of victims, witnesses, and suspects of crime are appropriately protected and will enable cross-border cooperation in the fight against crime and terrorism. [Dzikegielewska, 2017]

The GDPR law bestows us the opportunity to demand explanation for any instance of machine processing that uses our personal data. However, the GDPR is criticized for not providing the right to explanation concerning automated decision-making systems. [Dzikegielewska, 2017]

Since its early inception and approval of the European Union General Data Protection Regulation in 2016, it has been claimed that a 'right to explanation' of all decisions made by automated or artificially intelligent algorithmic systems are legally stipulated by the GDPR once it was enforced on May 25th, 2018. However, the enforceable actuality and the practicability of a right to explanation are doubted for several reasons. [Dzikegielewska, 2017]

Articles 13 upto 15 of the GDPR mandate that data subjects have the rights to receive relevant but precise information regarding the rationale involved as well as the the significance and anticipated repercussions of automated decision-making systems as right to information in contrary to detailed right to explanation. The obscurity, ambivalence and equivocation and restricted power of the 'right not to be subject to automated decision-making' contained in Article 22 (from which the ostensible 'right to explanation' stems) raises concerns over the preservation literally bestowed to data subjects. These predicaments reveal that the GDPR lacks scrupulous language as well as straightforward and comprehensible rights and protections against automated decision-making, and hence runs the risk of being ineffective.[Wachter et al., 2017]

2.2 Personal data

The GDPR wholly or partially applies to 'personal data', meaning any information relating to a person who can be directly or indirectly identified in particular by reference to an identifier.

The above explanatory description of personal identifiers account for personal data including name, identification number, location data or online identifier. These identifiers also include one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person reflecting changes in technology and the way organizations collect information about people. [Wachter et al., 2017]

A list of things that could be considered personal data, either on their own or in combination with other data includes: [Burri and Schär, 2016]

- Biographical information or current living situation including birth dates, Social Security numbers SSN, phone numbers and email addresses;
- Biometrics Information Looks, appearance and behavior including eye color, fingerprint, weight and character traits;
- Workplace data and information about education including salary, tax information and student numbers, private and subjective data including religion, political opinions and geo-tracking data;
- Health, sickness and genetics including medical history, genetic data and information about sick leave.

The personal data that are accumulated should be pseudonymised and/or encrypted. *Pseudonymisation* is the science of concealing data by replacing identifying information with artificial identifiers. Inspite of the fact that pseudonymisation is endorsed 15 times in the GDPR as being central to safeguarding the privacy and security of personal data, pseudonymisation has its shortcomings, which is why the GDPR also recommends encryption. Encryption is the art of obscuring in formation by replacing it by something that cannot be understood without a specific key. Thereby the entire information could be encrypted using encryption keys in such way that only authorized parties can get access to the information by decrypting it using decryption keys. Pseudonymisation grants access to anyone to view part of the data set. Encryption allows only approved users to have access to any part of the data set. These approved users can have access to the full data set by using the decryption keys. Pseudonymisation and encryption can be either used simultaneously or separately. [Spindler and Schmechel, 2016]

The General Data Protection Regulation explicitly recommends pseudonymization of personal data as one of several ways to reduce risks from the perspective of the data subject. It is helpful as a means for data controllers to enhance privacy. It makes it easier for controllers to process personal data beyond the original personal data collection purposes or to process personal data for scientific and other purposes.

Anonymization irreparably obscures any way of identifying the data subject.

Difference between pseudonymization and anonymization

Pseudonymization and anonymization are two distinct terms that are often confused in the data security world. With the advent of GDPR, it is important to understand the difference, since anonymized data and pseudonymized data fall under very different categories in the regulation.

Pseudonymization and anonymization are different in one key aspect. Anonymization irreversibly destroys any way of identifying the data subject. Pseudonymization substitutes the identity of the data subject in such a way that supplementary information is required to re-identify the data subject. Pseudonymisation swaps the identity of the data subject in such a way that extra supplementary information is required to re-identify the data subject.

Indirect re-identification is one of the concerning part of anonymization. An author writing and publishing books under pen name or pseudonym is using anonymity under a hidden unidentifiable name instead of his real name. when the pen name is resolved then we can

identify the real author.

Tokenization is a procedure of providing a a similar-looking token for each peculiar name and requiring access to supplementary information to re-identify the data. Tokenization is a mechanism which substitutes delicate data with unique identification symbols that maintains all the crucial information about the data without compromising its security. The main objective of tokenization is minimizing the amount of data a business needs to retain in the data base system. Tokenization is a prominent method for small and medium businesses to enhance the security of credit card and e-commerce transactions while reducing the cost and complexity of compliance with industry standards and government regulations.[Spindler and Schmechel, 2016]

Industry standard payment cards (PCI)[Diker Vanberg and Ünver, 2017] strictly prohibits the storage of credit card numbers on a retailer's point-of-sale (POS) terminal or storage of credit card details post transaction in its databases. In order to fulfill this requirement and to be PCI compliant,traders are obliged to implement costly end-to-end encryption systems or outsource their payment processing to a service provider who provides a "tokenization option". The service provider then processes the publication of the token value and reinforces the responsibility for retaining the cardholder data locked down. [Nyrén et al., 2014]

Merchants get a driver for the POS system by the service provider. The driver converts credit card numbers into randomly-generated values (tokens). Token can't be used outside the context of a specific peculiar transaction with that particular merchant since the token is not the primary account number (PAN). For instance, the token typically contains only the last four digits of the actual card number in a credit card transaction. The rest of the token consists of alphanumeric characters that represent cardholder information and data specific to the transaction in progress. [Nyrén et al., 2014]

Compared with older systems where credit card details were stored in traditional databases and exchanged freely over networks, tokenization is effective in deterring hackers from gaining access to the card holder data. Hypothetically tokenization can be used with delicate data of all kinds including bank transactions, medical records, criminal records, vehicle driver information, loan applications, stock trading and voter registration. [Nyrén et al., 2014]

Difference between a data processor and a data controller

A controller is the organization that decides the motives, conditions and means of the processing of personal data, whereas the processor is a unit which processes personal data

on behalf of the controller. The data processor processes personal data only on behalf of the controller. The data processor is usually a third party external to the company. However, in the case of groups of undertakings, one undertaking may act as processor for another undertaking.

The duties of the processor towards the controller must be specified in a contract or another legal act. For example, the contract must indicate what happens to the personal data once the contract is terminated. A typical activity of processors is offering IT solutions, including cloud storage. The data processor may only sub-contract a part of its task to another processor or appoint a joint processor when it has received prior written authorisation from the data controller. Below is a counter example that explains the difference between a controller and a processor

A brewery has many employees. It signs a contract with a payroll company to pay the wages. The brewery tells the payroll company when the wages should be paid, when an employee leaves or has a pay rise, and provides all other details for the salary slip and payment. The payroll company provides the IT system and stores the employees' data. The brewery is the data controller and the payroll company is the data processor.

Joint controllers

Your company/organisation offers babysitting services via an online platform. At the same time your company/organisation has a contract with another company allowing you to offer value-added services. Those services include the possibility for parents not only to choose the babysitter but also to rent games and DVDs that the babysitter can bring. Both companies are involved in the technical set-up of the website. In that case, the two companies have decided to use the platform for both purposes (babysitting services and DVD/games rental) and will very often share clients' names. Therefore, the two companies are joint controllers because not only do they agree to offer the possibility of 'combined services' but they also design and use a common platform.

Consent

The conditions for accord have been reinforced, and companies formerly using long illegible terms and conditions full of the abstruse technical vocabulary of the law, are no longer be able to do that anymore. Comprehensible, intelligible and easily accessible form must be provided to the data subject for requested consent with the grounds for data processing. The consent can be given to many purposes at the same time but this has to be clear to the data subject.

Consent should be given by a intelligible unequivocal, explicit act creating a freely given, specific, informed and implicit manifestation of the data subject's agreement to the processing of personal data relating to him or her, such as by a written announcement, including by electronic means, or an oral announcement. This could include ticking a box when visiting an internet website, adopting technical backgrounds for information society services or another announcement or conduct which noticeably shows in this context the data subject's affirmation of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore account for consent.

Consent should cover all processing activities implemented for the same motive or motives. When the processing has numerous motives, consent should be granted for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be lucid, precise and not needlessly distracting to the use of the service for which it is provided. [Burri and Schär, 2016].

2.3 GDPR articles

A legislation usually has more than one objective, intention, interpretation and implementation. No matter how meticulously formulated and context agnostic a law is, when encountered with a rapid and intense innovation, it gradually becomes obsolete and needs to be replaced by a more inclusive amended law that goes along with the current circumstantial reality. The European Data Protection Directive is an excellent example of such legislation. It might be arguable/disputable that the technological amendments brought on by the EU General Data Protection Regulation (GDPR) are nominal/numerical in comparison to the previous directive, but from a business perspective, the changes are remarkable and important. The companies have better direct incentive to protect personal data with the new regulation than with the old directive because companies may now have to pay severe fines for violating the legislation. [Calder, 2016]

The purpose of the GDPR is to safeguard EU citizens from data privacy breaches in an overwhelmingly data-driven world. In spite of the fact that the main principles of data privacy still hold true to the previous directive, many changes have been proposed to the administrative policies; the key points of the GDPR as well as information on the effects it will have on businesses are articulated in the broad legislation stipulated in articles of EU GDPR. The GDPR consists of 99 articles, grouped into 11 chapters, and an additional 171 recitals with explanatory remarks.

In this section, to get insight about the articles, we take a closer look at the first 8 ones. A few of the articles were already discussed in the previous sections of this thesis.

Chapter one focuses on *General Provisions* which includes the first four articles. *Article 1* is about *Subject-matter and objectives*. The security and protection of natural persons regarding to processing of personal data and relating to free movement of personal data are governed by rules set by the GDPR. Protection of freedoms of natural persons, particularly safeguarding personal data is the principal purpose of the regulation. Restriction nor forbidding of free movement of personal data will not be the reason related to the protection of natural persons and processing of personal data. [Diker Vanberg and Ünver, 2017]

Article 2 is about *Material scope*. Partial or complete processing of personal data by automated means and the processing of personal data that constitutes a filing system or are intended to be part of a filing system are governed by rules set by the EU GDPR.

Article 3 is about *Territorial scope*. Irrespective of the whereabouts or territories processing of personal data takes place, the regulation sets rules that are applied to controllers and processors. These rules concerns controllers and processors with the context of activities and establishment within or outside of the union.[Diker Vanberg and Ünver, 2017]

Article 4 is about *Definitions*. It gives detailed explanatory definitions about personal data, processing, restriction of processing, profiling, pseudonymization, filing system, controller, processor, recipient, third party, consent, personal data breach and other important issues.[Diker Vanberg and Ünver, 2017]

Chapter two of GDPR is about *Principles* which includes *7 Articles, Article 5 - Article 11* about principles relating to processing of personal data.

Personal data shall be : [Diker Vanberg and Ünver, 2017]

- Processed lawfully, fairly and in a transparent manner;
- Collected for specified, explicit and legitimate purposes;
- Adequate, relevant and limited to what is necessary;
- Accurate and, where necessary kept up to date;
- Retained only for as long as necessary;
- Processed in an appropriate manner to maintain security and accountability.

Article 6 is about *Lawfulness of processing*. It lists several requirements for the processing to be accepted as complying to the regulation and lawful. The processing of personal data should be secure against accidental loss and destruction or damage. Consent for specific purposes of personal data must be granted by the data subject as a preliminary requirement. However, there are also other specific circumstances where consent of the data subject is not required so that the controller can comply with legal obligations. Processors must operate under a legally binding contract and controllers are responsible for ensuring processors comply with contractual terms for processing information.[Diker Vanberg and Ünver, 2017]

Article 7 is about *Conditions for consent*. The data subject grants consent to the controller upon request for processing of their personal data. Withdrawal of consent at any time they wish as well as the processor to give access for the data subject upon request as well for what purpose and how their personal data is used in the processing by the controller. Whether the agreement is verbal or written it shall be considered binding. Any infringement or violation by the controller will be treated based upon the binding agreement.[Diker Vanberg and Ünver, 2017]

Consent must be clear and affirmative. The controller as well as the data subject must be able to demonstrate that consent was given. Silence or inactivity does not constitute consent. Written consent must be clear, intelligible and easily accessible, otherwise it is not binding. To withdraw consent at any time easily either by the processor, controller and data subject must be granted,it must be as easy to withdraw the consent as it is to give it.[Diker Vanberg and Ünver, 2017]

Special conditions apply for child (under 16 years old) to give consent. Explicit consent must be given for processing sensitive personal data such as race, ethnic origin, gender. Specific circumstances allow non-consensual processing such as to protect vital interests of the data subject. [McCall, 2018]

Article 8 is about conditions applicable to child's consent in relation to information society services. The processing of personal data of a child will be legitimate if the child is under 16 years old related to the offer of information society services directed personally to the child. If the child is below the age of 16 years, the authorized parental responsibility or guardian representative should give consent so that processing is legit. However, each member state may provide a lawful lower age limit for processing purposes, but the lower age limit will not be below 13 years though. [McCall, 2018]

We have presented first 8 articles. There are still 91 more but discussing all of them would

take too much space from the thesis. Some other articles would, however, be discussed later in the thesis when a specific topic is under discussion.

3 Analysis and details of GDPR

The GDPR is criticized by concerned experts for its unpragmatic and overambitious objectives. The criticism is that GDPR is based on three fallacies. The delusional misinterpretation that data protection law can give individuals control over their data is the first fallacy. The misconception that the reform paraphrases the law, whereas in fact it makes compliance even more complicated is the second fallacy. The third poor logic or fallacy is the speculation that data protection law should be inclusive and complete, which extends data protection to the point which makes it unintelligible law in the books. [Albrecht, 2016]

However, after the pragmatic implementation of the GDPR, results are different from the expectations, illusions and delusions envisaged before experiencing the practicalities. Most member states have set up the necessary legal framework, and the new system strengthening the enforcement of the data protection rules is falling into place. [Voss, 2017]

Meanwhile citizens, data subjects are getting more awareness about their rights, businesses are developing habitual culture of acquiescence, compliance and concession to the set rules. Simultaneously, propensity of convergence toward high data-protection and security guideline standard measures is progressing at global scale. However, the evaluation also highlights specific areas of concern. The Commission warns that it will utilize all the tools at its disposal, including infringement procedures to ensure member states comply with GDPR.[Voss, 2017]

There is a saying that personal data is the new oil of the internet and the new currency of the digital world. In European perspective, the right of privacy and the data protection right are considered to be profoundly different from each other. The emphasis of data protection right is on the fairness and reasonableness of the personal data utilization. [Voss, 2017]

The GDPR can be considered as a data administration structure. The GDPR recommends that companies to focus meticulously about data and have a clear procedure for the collection, usage, and destruction of the data. Some businesses that are not especially data-intensive in their corporate structure may be obliged to increase the utility of data in their activities throughout compliance to the GDPR. The GDPR will be an opportunity for some businesses to evaluate more rigorously the importance of their data, other

businesses will use GDPR as an opportunity to more accurately evaluate the value of their data, transforming the data to a tactical asset, on the same magnitude as companies view their patent portfolio or copyrights. Data privacy and information privacy are discussed in European law interchangeably. They both are concerned with the collection, utilization and disclosure of personal information. They both refer approximately to the same concept. [Voss, 2017]

Fundamental rights and other public interests might encounter conflict with the GDPR data privacy rights, such as transparency of governance, freedom of speech and freedom of data movement as well as archiving purposes of data processing. Freedom of speech is equally important and fundamental in European law as data privacy that are expected to go along in parallel. The balance between data protection and freedom of speech interests are the requirements of the GDPR member states. These requirements for instance state that the GDPR do not apply when the purpose of data processing is for academic, artistic or literary expression. [Tikkinen-Piri et al., 2018]

Most business standard functions comply with legit interests. Website publishers are allowed to stockpile or accumulate IP addresses of website visitors for a short period, if that complies with security requirements, for instance, for prevention of fraud such as money laundering. Storing customer's information such as name and address does not necessarily infringe GDPR privacy rules, and for instance, pizzeria that stores customer's information has a valid interest in promoting its own business. The pizzeria passes the compliance requirement of the GDPR balancing test prescribed by the legitimate interests provision. [Tikkinen-Piri et al., 2018]

We take article 13 as an example and discuss it to get a highlight of the contents of the articles. It is also one of the most contentious and criticized articles. Article 13 is one of the 99 articles of the GDPR which concentrates on information to be provided to the owner where personal data are collected from the data subject. The data controller is obliged to provide their contact details to the data subject and the legal basis and purpose of processing the information.[Diker Vanberg and Ünver, 2017]

The internet trend that uses still images from popular television shows or films and combines them with user generated content to create topical humor is known as meme. Article 13 is occasionally called the meme ban. [Burri and Schär, 2016]

Article 13 is section of the directive of GDPR that centers on the use of protected content by 'information society service providers' (ISSPs), which store and give access to material uploaded by users. Creating mash-ups and remixes from original musics and sharing it

online became history on the internet after article 13 approved and passed.

Technology companies already have different kinds of filters to prevent certain kinds of content from appearing online. Implementing such system into the way that article 13 recommends spontaneously raises numbers of questions. This is because 'copyright' is such a broad term and should not be used against free speech. This applies to memes, parodies, travesties, clips of people at sporting events, YouTube creators providing reviews of movies and more. We are now entering the world of censorship, completely changing the way that the Web works. Fair use of copyrighted material is encountering conflict with this law. [Koops, 2014]

The biggest criticism about article 13 is from the largest video sharing platform YouTube. This is not as such surprising as this website relies on user-generated content and will be directly affected by article 13. YouTube which is a faction owned by Google was not the only one fighting against article 13. In June of 2018, a Silicon Valley lobbying group called CCIA published an open letter against the GDPR directive. [Burri and Schär, 2016] This group includes companies such as Facebook, eBay, Amazon, and Netflix. It is also worth noting that Git Hub is opposing the law even though this company (along with Wikipedia) is explicitly excluded from companies affected by article 13. The immediate and simplest solution to alleviate the ramifications of article 13 especially sustaining free speech and experiencing the internet as it is today resolving copyright infringement issues is Virtual Private Network. [Burri and Schär, 2016]

Increased territorial scope(extra-territorial applicability)

Stretched jurisdiction of the GDPR is conceivably the substantial change to the data privacy regulatory landscape which is applicable to all business entities that process personal data of EU residents irrespective of the location these companies reside in. Formerly, however, territorial applicability of the regulation was ambivalent or equivocal referred to data process ' in context of an establishment'. The applicability of the GDPR is eloquently elaborated in an intelligible and plain language unequivocally/unambiguously that it will apply to controllers and processors regardless of their residential location that are processing personal data. A controller or processor not established in the EU but still processes personal data of data subjects of EU should also abide by the GDPR whether offering goods and services to the EU citizens irrespective of whether payment is required and the monitoring of behavior that takes place within the EU. Any Non-EU businesses will have to appoint a representative if their operation involves processing the data of EU citizens.[Diker Vanberg and Ünver, 2017]

3.1 Data subject rights

People residing in the EU in their different capacities as consumers, citizens and so forth are granted a range of specific data subject rights they can execute under specific conditions but with a few exceptions. Enabling the exercise of these rights is obtained by complying with GDPR among other means. Overview of 8 fundamental data subject rights and additional citizen rights in specific circumstances are discussed below. There are no absolute data subject rights as there are conditions and exceptions, but there are also other rights to keep in mind. The right of freedom of expression and information, for instance, can have an impact with regards to the right of erasure. [Burri and Schär, 2016]

Breach notification

Breach notification under the GDPR will become imperative in all EU member states where a data breach is likely to "result in a risk for the rights and freedoms of individuals". Within 72 hours of first having become aware of the breach, a notification must be made. Data processors will also be required to notify their customers, the controllers, "without undue delay" after first becoming aware of a data breach. [Burri and Schär, 2016]

The data subject's right to rectification

When personal data are inaccurate, then controllers need to correct them indeed (GDPR Article 16).

The data subject right to restriction of processing

The right of the consumer or whatever you call the natural person under the scope of the GDPR, to limit the processing of his/her personal data. (GDPR Article 18).

The right to be informed

In general, the GDPR requires controllers and processors to inform data subjects on several matters. Providing intelligible and accurate information is an important role in many regards. The GDPR Article 19 wants consumers to know, the controller must inform recipients who got these data, where feasible and then the data subject also has a right, to ask who are all these recipients who got to see the data.

The right not to be subject to automated decision making

It is a right of data subject not to be subject to be subject to a decision based entirely on automated processing, such as profiling, which results enforceable impacts concerning him or her or consistently and enormously affects him or her, is the right of data subject.

Right to access

To obtain from the data controller assurance as to whether or not personal data concerning them is being processed is the right for data subjects. Providing a copy of the personal data, free of charge, in an electronic format to the data subject is the duty of controller. Regarding data transparency and empowerment of data subjects, this is a fundamental change. [Burri and Schär, 2016]

Right to be forgotten

The right to be forgotten, also known as data erasure, authorizes the data subject to have the data controller erase his/her personal data, to discontinue extra publication of the data, and to make third parties cease processing of the data. The requirements for erasure, as indicated in article 17, state about the data no longer being relevant to original purposes for processing, or a data subject withdrawing consent. This right requires controllers to compare the subjects' rights to "the public interest in the connection with the data" when considering such requests. [Burri and Schär, 2016]

Data portability

The right for a data subject to claim the personal data concerning them, which they have formerly granted in a 'machine readable as well as commonly used format' and the right to pass on that data to another controller is known as data portability.[Diker Vanberg and Ünver, 2017]

Privacy by design

Privacy by design which is being included as a procedural requirement in the GDPR has existed for years as a concept. The core idea of privacy by design is the inclusiveness of data protection from the beginning of the systems designing rather than being an addition. Particularly the law requires the controller to implement relevant organization and technical standards effectively in order to comply with the the regulation requirements and protecting data subjects rights. Data minimization which is holding and processing only the data that are necessary for the accomplishment of duties as well as limitation of personal data access for those requiring to execute the processing are the mandatory rules of Article 23 for controllers. [Burri and Schär, 2016]

The GDPR specifies six legal justifications for data processing: The data subject has consented to the data processing. The data processing is necessary for a contract with the data subject. There is a law mandating the data processing (e.g. tax law requires companies to keep certain records). Data processing is necessary to protect the life of a data subject (e.g., the data subject is unconscious after a car accident, and the hospital needs to know

from the data subject's family doctor whether the data subject uses certain medication). Data processing happens for a public task (e.g. the tax office gathers certain data, such as people's tax returns, to fulfill its tasks) and last but not least when the interests of the data controller prevail over the interests of the data subject. [Burri and Schär, 2016]

Data protection officers

Controllers are obliged to inform to the local Data Protection Acts DPAs about timely and accurately their undertaking concerning data processing. This might be a cumbersome bureaucratic procedure for most companies as the notification prerequisites varies in each and every member country of the EU. Additionally there is no need to provide registrations information to the local Data Protection Acts about each activity. However, companies are required to keep track of their activities internally by documenting their data processing activities. Hiring data protection authority is compulsory for controllers and processors which execute regular and constant large scale operation of data subjects, which monitor special categories of data such as criminal offences convictions. The employment of the data protection officer must be compliant to the required expertise level from the GDPR concerning knowledge regardless of whether the duty is outsourced to an external proficient professional or managed by regular internally hired expert. [Burri and Schär, 2016]

3.2 GDPR penalties for non-compliance

To implement a uniform data protection law on all EU members is the core purpose of the GDPR, so that each member state no longer needs to write its own data protection rules and these laws are uniformly implemented across the entire EU. It is vital to comprehend that any company that undertakes transaction of goods or services to EU residents, regardless of its location, is subject to the regulation. Eventually, the GDPR will have an influence on data protection requirements globally [Burri and Schär, 2016].

The regulation imposes strict legal repercussions on companies resorting to violations and trespassing the ethics and etiquette of customers' data handling. The lack of complacence and conformity with the new regulation imposes tremendous monetary fines as well as severe sanctions on organizations. The financial fines scale up to 20 million euros or alternatively 4% of their annual turnover, the higher amount between the two alternatives is considered as the upper limit fine. These penalties mentioned are the maximum amount of monetary fines that can be inflicted for the most serious infringements, e.g., not having sufficient customer consent to process data or violating the core of privacy by design concepts. There is a tiered hierarchical approach to these fines e.g a company can be fined 2% for not having their records in order, not notifying the supervising authority and data subject about not conducting impact assessment or a breach. These rules unequivocally apply to both controllers and processors which means that 'clouds' are not exonerated from EU GDPR enforcement. [Gilbert, 2011]

The GDPR has significantly increased penalties for non-compliance compared to the former Data Protection Directive. All companies operating in the EU, handling personal data of citizens of the EU have to abide by standard rules calibrated by the GDPR. The regulation gave supervisory authorities more capacity than the prior legislation in many forms and shapes. The authorities include performing audits thereby ensure compliance, give warnings during non-compliance, impose deadlines on reform activities of companies, preclude transmission of data to other countries, stipulate the erasure of data, issue larger fines than the Data Protection Directive. Furthermore supervisory authorities have power on data controllers and processors and can penalize them during violations. Fines imposed by supervisory authorities for non-compliance or violations depend on the circumstances of each case. [GROOT, 2017]

Determination

Fines are regulated by individual member state supervisory authorities (see article 83.1).

Eleven criteria to be used to determine the amount of the fine on a non-compliant firm are listed below:[Diker Vanberg and Ünver, 2017]

- The type of infringement: this is associated with the victims who suffered from the violation, the purpose of the data processing their personal information was used for as well the time length or duration the infringement lasted
- Intention: this is concerned with whether the violation or infringement was inflicted purposefully or irresponsibly with negligence
- Preventive measures: envisaging any damage expected to affect personal data of the data subject thereby the effort the firm has made. Advance organizational and technical preparation to avoid compliance infringement or violation
- Mitigation: procedural guidelines and actions followed to minimize or mitigate the damage imposed upon data subjects
- History: (see article 83.2e) previous infringements which include violations not only under the GDPR but also the data protective directive (see article 83.2i) and the prior administrative measures taken including warnings, sanctions and fines imposed as corrective procedural guidelines
- Cooperation: the extent to which the company has been cooperating with the supervisory authority officials to alleviate the violation.
- Data type: the impacts imposed on the types of data and special categories of data
- Notification: the endeavors the firm exerted to report the violation proactively by itself or if the notification automatically generated the information
- Certification: if the firm is abiding by approved certifications or codes of conduct. Where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures
- Other: other exasperating or alleviating circumstances resulting from the infringement may include monetary repercussions on the firm.

3.3 Best practices for GDPR

Compliance to the GDPR since May 2018 must be the duty of all organizations from small-scale to medium-sized businesses, companies and large enterprises. The organizations have to create awareness about the fundamental requirements of the EU GDPR. Advance preparation to implement the data protection policies and solutions will help companies to be in a better position to accomplish GDPR compliance. For this purpose, the first step in complying with GDPR is to appoint a data protection officer to develop a data protection program that complies the GDPR requirements.[Burri and Schär, 2016]

General Data Protection Regulation applies to businesses not only in the EU but also all businesses selling goods or services to EU citizens. Providing customer data protection and trust and complying with EU GDPR requirements will benefit immensely businesses thereby averting huge fines.

4 Relevant technologies

There are many technologies associated with GDPR either to circumvent the rules and misuse it by bad actors or important technologies that are helpful to reinforce the regulations and implement them effectively. In this chapter we will discuss some of these technologies. These technologies include but are not limited to Virtual Private Network(VPN), Encryption, Anonymization, Pseudonymization and Block Chain.

4.1 Virtual private network

A virtual point-to-point connection through the use of dedicated connections, virtual tunnelling protocols, or traffic encryption is considered as establishing a virtual private network. Public internet availing VPN can grant certain benefits similar to a wide area network (WAN) can provide. Remote access of resources available within the private network is another benefit from a user perspective. VPN works both in IPv4 and IPv6 versions. (see Figure 4.1).[Burri and Schär, 2016]

VPN applications let users to connect to a server located in some other country where they are, and therefore browse the web like they were physically located in that other country. This has already happened during major events such as the FIFA World Cup and similar. As a result of article 13 enforcement, VPN is necessarily required at all times which in turn result steady costs. [Burri and Schär, 2016]

There is no need of approval from internet service providers or regional registry to use Private network addresses since they are not attributed to any specific organization, therefore anyone may use these addresses. However, IP packets addressed from them cannot be routed through the public Internet. Virtual Private Network technology was developed to allow remote users and branch offices to access corporate applications and resources. To ensure security, the private network connection is established using an encrypted layered tunnelling protocol and VPN users utilize authentication methods, including passwords or certificates, to gain access to the VPN. Transactions could be secured in other applications using VPN. Virtual private network could also be used to circumvent geographical restrictions and censorship, or to connect to proxy servers to protect personal identity and location in order to stay anonymous on the internet. However, some internet sites

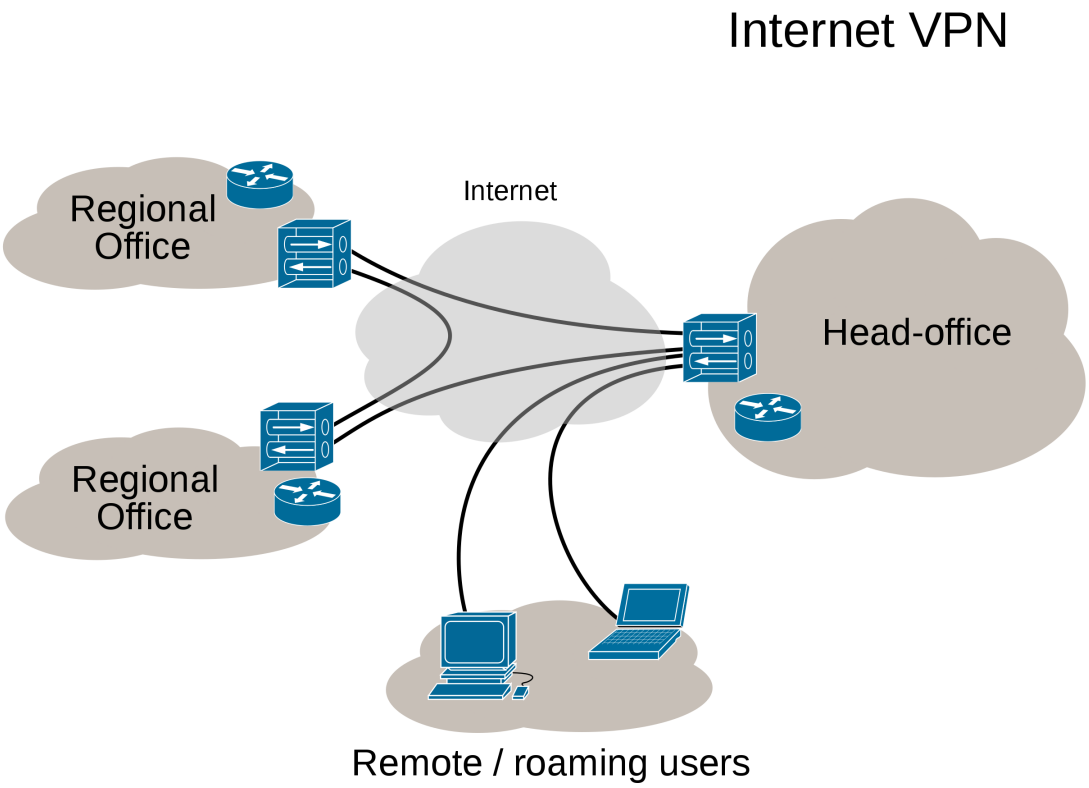

Figure 4.1: Virtual Private Network
[Gupta et al., 2001]

block access to known VPN technology to prevent the circumvention of their geographical restrictions. Many VPN providers have been developing strategies to get around these barriers (see Figure 4.2). [Berberich and Steiner, 2016]

Figure 4.2: YouTube Video Not Available In Your Country

4.2 GDPR and data security

Email as an important subject for GDPR regarding data privacy and protection, security of personal data of individuals otherwise known as data subjects. Data Subjects own the private information. Email mailbox indeed contains important details such as names, email addresses, attachments and personal conversations. This data is governed by the strict requirements of the GDPR stipulating organizations to abide by all forms and shapes of data protection. The regulation also reinforces consent and personal data privacy rights of data subjects. [Tikkinen-Piri et al., 2018]

The GDPR does not allow exceptions to any organization regarding data privacy protection rights. Business entities, micro finance enterprises, charities are all mandated to respect the GDPR rules while handling personal information of EU citizens and residents. This includes organizations not in the EU but which offer goods or services to people living in the EU GDPR territorial scope . The main purpose of the GDPR is securing personal data and making it easy for people to control over their data. Those who violate the rules

are penalized with fines according to the specified scales in GDPR plus compensation for damage. The GDPR requirements regarding email are centered around email marketing and spam. It includes encryption and email safety which are very important for GDPR compliance. [Absalom, 2012]

Organizations must always meticulously consider new or existing products or services regarding their implications to data privacy protection rights stipulated by the GDPR requirements "data protection by design and by default". Principles of data protection that everyone must adhere to are listed in Article 5 of GDPR which includes implementation of appropriate technical measures for security of personal data. The main examples mentioned regarding technical measures include encryption and pseudonymization that are essential in minimizing damages inflicted during data breach. Numerous companies now offer end-to-end email encryption as the technology has rapidly sophisticated. An example of this technology is cloud based secure email. ProtonMail, developed by CERN and MIT scientists, is a practical example of encrypted secure email. The developers claim it is the largest secure email service. Although encryption is not always mandatory, organizations are required to develop appropriate data security practices. [Lindqvist, 2017]

The right to be forgotten, also known as erasure of data, imply permanent permanent deletion of data that is no longer needed for the purposes for which this personal data are processed. Retaining the data only as long as necessary is one of the six important principles of the GDPR. The controller has the obligation to give information about the erasure of personal data concerning a data subject without undue delay. However, there are some exceptions to this requirement, such as the public interest. [Lindqvist, 2017]

The erasure of unneeded personal data is required by the GDPR. This law also requires organizations to periodically review their email retention policy. The objective is to reduce the amount of data employees store in their mailboxes. Many people never delete emails due to plenty of reasons such as possible future litigation requirements and for record of activities. However, retaining more data exposes us for greater liability if a data breach occurs. Under the GDPR organizations are required to have a policy that balances legitimate business interests versus data privacy and protection obligations. Email data deletion under the GDPR, data erasure under the GDPR is technically automated in a certain level. Some email services such as ProtonMail have options to designate expiring time duration after which email messages are marked for deletion. Following email retention strategy significantly lowers GDPR exposure. [Koops, 2014]

Under the GDPR article 5, it is required that using personal data is legal only if it is allowed

in one of the six legal justifications such as lawfulness, fairness and transparency. The use of people's data must be fair to the data subject and it must be based on transparent and unambiguous communication with the data subject.

There are six "legal bases" for processing (collecting, storing, using , etc.) people's data. These are listed in Article 6. The first is consent, which must be obtained unambiguously and after a full explanation of what you plan to do with the data. Specifically: consent must be "freely given, specific, informed and unambiguous."The 2nd, 3rd, 4th and 5th legal bases are all about cases where processing the data is necessary for various reasons such as performance, legal obligation or protection of vital interests of the data subject.

Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

Consent request for processing data must be "clearly distinct from the other matters" and presented in"clear and plain language." Data subjects can withdraw previously given consent whenever they want, and entities (organizations, companies etc.) you have to honor their decision. It is not possible simply to change the legal basis of the processing to one of the other justifications. Permission from parents is required to process data

of children under age of 13. The sixth legal basis is to have a "legitimate interest"to process the person's data. Although the term is vague and could apply to a broad range of situations, you may have a hard time relying on this basis because the legitimate interest may override "fundamental rights and freedoms of the data subject". Moreover, it remains to be seen how regulators and the courts will interpret this basis. [Lindqvist, 2017]

The ePrivacy Directive, specifically Article 13 of the GDPR, grants organizations the opportunity to use personal data legally for marketing purposes, as part of the contractual basis of the GDPR. An organization may use electronic contact details of data subjects for direct marketing communications to sell goods or services provided that the customers are given the opportunity to clearly and distinctly object in an easy manner according to part 2 of article 13. In particular, this means that an organization can legitimately send marketing emails about the services or goods they provide as long as in every communication, they inform the customers about the option to unsubscribe at any time the customer wants in every communication. People had the expectation that once the GDPR is passed, it will be the end of email marketing and spam, but it has been neither yet. Although spam has always been against the terms of use of most email providers, those sending unsolicited and malicious mass emails will continue to send them. [Lindqvist, 2017]

Generally speaking the GDPR is pro customer but at the same time not anti business. It does not prohibit email marketing by any means. The principle is based on the fact that good marketing adds value to the recipient and promotes what the customer wants to receive. The GDPR, however, emphasizes on the terms of consent thereby requiring organizations to request an affirmative opt-in and opt-out communications making it easy for people to change their mind at any time they want. The violation of the GDPR requirement happens whenever a marketing email does not present the option to unsubscribe or is sent to someone who never signed up for it or advertises business the recipient had previously had withdrawn consent.

The other important aspect of the GDPR regarding email is security. The GDPR mandates that personal data should be protected from accidental loss, damage or destruction using appropriate technical measures organizations are required to be equipped with.

Ninety-one percent of cyber attacks originate from phishing emails where hackers attempt to gain an unauthorized access to an account or device via malicious malware or fraudulent deception. Therefore it is dangerous to open links and attachments from unknown sources. The more detrimental part of granting access to hackers or an unauthorized entities is that once they gain access to other devices, it is quite easy to access others which implies that

mistake by one employee compromises a massive amount of data. While organizational measures have to do with internal policies, management and training, email encryption is a technical measure against data breaches. If organizations cannot show that they have implemented the appropriate technical and organizational measures, then they are subject to EU GDPR fines and compensations to the data subjects. [Lindqvist, 2017]

In order to avoid liability, organizations need to educate their employees about email safety, basic procedures like requiring two-factor authentication which are helpful in protecting data privacy and enhancing compliance with the GDPR.

4.3 Authentication, authorization and accounting

With the GDPR identity requirements are expanded compared to the Data Protection Directive it replaces, the identity requirements for organizations are more expanded in GDPR than the Data Directive. Although it is not mandated by GDPR to use two factor and multifactor authentication security procedures, if the data subject is irresponsibly negligent using weak, static and easily breakable or easy to compromise passwords, the data subject will be held ethically accountable for the irresponsibility and negligence for any data breach that occurs as a result consequently not as a monetary fine though.

Auditors heavily and constantly scrutinize the use of weak, static and easily-compromised credentials wherever they exist in the mean time. If the GDPR rules are read meticulously, they suggests that the use of simple, static and easily-compromised passwords is forbidden, and auditors will hold users having weak credentials accountable. Although the GDPR does not mandate it, the use of two-factor and multifactor authentication solution is recommended. Smart organizations are considering to use the opportunity refreshing technology to get rid of passwords entirely. [Weir et al., 2017]

Any organization operating, storing or processing data within the European Union needs to be in compliance with GDPR. That means if an organization is not located in the EU, but this organization runs data through an EU data center or store information on EU customers with personally identifiable information inside the EU, the organization need to be in compliance with the law.

The popular web browsers and manufacturers of security tokens are implementing authentication standards. Personal computers and mobile phones are shipping on-device authenticators that are interoperable with these updated web browsers. This emerging

open standards ecosystem for user authentication, complete with third-party certification programs for independent validation, is well positioned to reduce the risk and costs of GDPR compliance around the world.

Authentication, Authorization and Accounting (AAA) form a system for tracking user activities on an IP based network and controlling their access to network resources. The AAA system is often implemented as a dedicated server. The term "AAA" is also used to refer to AAA dedicated server or AAA protocol.

Authentication, authorization, and accounting is a term for a framework for intelligently controlling access to computer resources, enforcing policies, auditing usage, and providing the information necessary to bill for services. These interrelated processes are considered important for effective network management and security. The three A's Authentication, Authorization and Auditing provides protected access to users on different privilege levels.

Authentication provides a way of reliably identifying a user, typically by having the user enter a valid user name and valid password before access to the system resources is granted. The process of authentication is based on each user having a unique set of criteria that needs to be verified. The AAA server compares a user's authentication credentials with user credentials stored in a database. If the credentials match, the user is granted access to the network. If the credentials do not match, authentication fails and network access is denied. [Tankard, 2016]

Authentication refers to unique information from each system user, generally in the form of a user name and password. System administrators monitor and add or delete authorization of users in the system.

Authorization refers to the process of adding or denying individual user access to a computer network and its resources. Users may be given different authorization levels that limit their access to the network and associated resources. Authorization determination may be based on geographical location restrictions, date or time of day restrictions, frequency of logins or multiple logins by single individuals or entities. Other associated types of authorization service include route assignments, IP address filtering, bandwidth traffic management and encryption. [Tankard, 2016]

Following authentication, a user must gain authorization for doing certain tasks. After logging into a system, for instance, the user may try to issue commands. The authorization process determines whether the user has the authority to issue such commands. Authorization is the process of enforcing policies: determining what types or qualities of

activities, resources, or services a user is permitted. Usually, authorization occurs within the context of authentication. Once you have authenticated a user, they may be authorized for different types of access or activity.

Accounting refers to the record-keeping and tracking of user activities on a computer network, measures users resource utilization and consumption during access. For a given time period this may include, but is not limited to, real-time accounting of time spent accessing the network, the network services employed or accessed, capacity planning and trend analysis activities, network cost allocations, billing data, amount of system time or the amount of data a user has sent and/or received during a session, login data for user authentication and authorization, and the data or data amount accessed or transferred.

Authentication, authorization, and accounting services depend on each other. They are often provided by a dedicated AAA server, a program that performs these functions. A standard protocol by which network access servers interface with the AAA server is the Remote Authentication Dial-In User Service (RADIUS).[Vandenbroucke and Olsen, 2013]

Examples of AAA protocols:

- Diameter, a successor to Remote Authentication Dial-In User Service (RADIUS [Nelson, 2011]
- Terminal Access Controller Access-Control System (TACACS) refers to a family of related protocols handling remote authentication and related services for networked access control through a centralized server. It is common to UNIX networks [Finseth et al., 1993]
- Terminal Access Controller Access-Control System Plus (TACACS+) a proprietary Cisco Systems protocol that provides access for network servers, routers and other network computing devices. [Amin et al., 2004]

4.4 Confidentiality, integrity and availability

The key security principle of data protection law under the GDPR is implementing appropriate technical and organizational measures for protecting and securing personal data preventing data breach. This implementation includes risk analysis, organizational policies, physical and technical measures. These security measures must maintain confidentiality,integrity and availability preventing any data breach compromises of personal data

processed in system services. During any physical or technical hazard, organizations must be able to restore access and availability of resources in a timely manner as a result of these effective measures implemented. Encryption and pseudonymisation are appropriate measures organizations must consider as part of the technical measures. [McDowell, 2019]

Cyber security is the procedure or state of protecting and recovering networks, devices and programs from any type of cyberattack. Cyberattacks are an emerging threat to organizations, employees and consumers. These attacks may be launched to access or destroy sensitive data or extort money. They can, in effect, destroy businesses and damage financial and personal lives, particularly if someone is the victim of identity theft.

Cyber security is an important part of the internet. Reconnaissance, Identity theft, Sybil attack, denial of service attack, phishing attack, spam, virus,malware, man in the middle attack, eavesdropping, cyber bullying, stalking, defamation,embezzlement, vandalism etc are cyber attacks that should be alleviated using security measures.

Confidentiality, integrity and availability are parts and parcels of ensuring personal data protected against data breaches. Confidentiality measures the secrecy of the sensitive information stored and who has access to this confidential information. Medical history and bank card details are examples of data that could impose serious security vulnerability threat and probably financial as well as psychological damages if fall under the wrong hands and information is leaked to any unauthorized entities.

Integrity is the authenticity of the information, which means the right information is transmitted between the sender and the receiver without any alteration or intrusion changing the message on its way. Certificate authorities give digital signature service to verify the authenticity using cryptographic methods based on private and public key infrastructures. Availability means authorized personnel are able to access information whenever wanted by the authorized personnel. While unauthorized access is denied, authorized access should be available whenever and whoever needed it. [Kennedy and Millard, 2016]

Computer components susceptible to security vulnerabilities are the hardware, software and data as well the communications among them are exposed to attacks. Routing protocols should also ensure the confidentiality, integrity and availability of routed information. The attackers are always endeavouring to devise mechanisms to compromise computer systems and exploit resources. Therefore, security is an endless process as far bad actors are perpetuating along with these useful technologies, attacks may happen at any moment. In communication systems and routing protocols, security is a delicate issue. This means, no matter how technological advancement is sophisticated, bad actors will find a loophole

to hack and abuse the technology. Latest technical measures in conjunction with secure cryptographic systems should be implementable to prevent cyber security threats and vulnerabilities. It is crucial for cybersecurity to avoid underestimating attackers and always do routine ethical hijacking to identify susceptibilities thereby securing the system all the time. Giant companies like FaceBook, Microsoft, Google and many others pay millions of dollars for ethical hackers who find loopholes in their systems. This is because security is very important part of their systems. This is because the little loophole may result in loss of millions of dollars if attackers find a way through the system. [McDowell, 2019]

The CIA triad confidentiality, integrity and availability are intended to manage organization information security policies. In this regard, confidentiality is a set of rules that restricts access to information, integrity is the confirmation that the information is trustworthy and accurate, and availability is a guarantee of reliable meantime access to the information by authorized people.

Measures implemented to safeguard confidentiality are intended to prevent leakage of sensitive information into wrong hands as the same time making sure the right people have access to it view it and access is only restricted to the authorized right people. Depending on the amount and type of damage inflicted because of an unauthorized unintended access, stringent measures should be implemented accordingly. [McDowell, 2019]

Strong passwords and password-related best practices and social engineering methods further training aspects are important to prevent distorting data-handling rules and their potentially catastrophic consequences. Training is helpful to familiarize users with risk factors and how to guard against them.

Data encryption is another example of ensuring confidentiality. Other standard procedures include, user IDs, two factor authentication, biometric verification, security tokens, key fobs and soft tokens. Additionally precautions could be taken by users such as minimizing the number of places where the information is stored and the number of times it is actually transmitted to complete a required transaction. For extremely sensitive documents, extra precaution measures should be implemented such as storing only on air gapped computers, disconnected storage devices and highly sensitive information should be stored only in hard copy form.

Breach of confidentiality is an example of compromising integrity of data on communication channel during transit. Therefore ensuring that access to data is only granted to authorized people and unauthorized people are denied access to resources, maintaining consistency, accuracy and trustworthiness are parts and parcels of data integrity over its

entire life cycle.

File access permissions and user access control privileges, version control to prevent erroneous changes or accidental deletion by authorized users could be measures taken to reinforce integrity and confidentiality. Non-human-caused events such as an electromagnetic pulse (EMP), server crash and other unprecedented catastrophic incidents should be detected by methods implemented. Check sums, even cryptographic check sums could also be used for verification of integrity. Backups or redundancies must be available to restore the affected data to its correct state. [McDowell, 2019]

Rigorously perpetuating all hardware, conducting hardware repairs promptly when needed and preserving accurately functioning operating system environment that is free of software conflicts are some of the best practice measures to ensure availability. To have upto date latest systems and upgrades is very important measure. Preventing the occurrence of bottlenecks and providing adequate communication bandwidth is also important. Redundancy, fail over, high-availability clusters can mitigate serious consequences when hardware failure do occur. However, because of privacy, GDPR restricts availability. [Diker Vanberg and Ünver, 2017]

Adaptive disaster recovery mechanism is essential for this purpose. Data backups should be stored in waterproof, fireproof and geographically-isolated location. Malicious attacks such as denial of service (DoS) attacks and network intrusions that cause downtime and unreachability in data access could be prevented by taking extra security precautions such as firewalls and proxy servers.

The concepts of AAA and CIA are interrelated in many ways. Some examples of these relations are mentioned in the following. The integrity in CIA includes authenticity of the data while authentication in AAA ensures that only authenticated users can get access to the data. Availability in CIA requires that authorized users should have access to the data while authorization in AAA provides means to define who the authorized users are. There is a similar situation with confidentiality in CIA that requires only authorized people to have access to the data.

5 Permanent deletion of data

One of the measures required reinforcing the right to be forgotten in the online environment is broadening the law so that the controller who disclosed personal data to the public is mandated to inform the processors. This makes the right to erasure a more strict law. The processors which are processing personal data are required to erase any links to, or copies or replications of those personal data.

The controller should take appropriate measures, availing important technology framework and other relevant means available to the controller, to inform the processors which are processing the personal data upon the data subject's request.[Lambert, 2016]

Some examples of secure data deletion obligations and data that can not be immediately deleted are listed below.

- Carol has joined a social networking site. After a while, she decides to leave the networking site. She has the right to ask the company to delete the personal data belonging to her;
- A new bank offers good home loan deals. Bob is buying a new house and decides to switch to the new bank. He asks the 'old' bank to close down all accounts and requests to have all his personal details deleted. The old bank, however, is subject to a law obliging banks to store all customer details for 10 years. The old bank can not simply delete his personal details. In this case, he may want to ask for restriction of processing of his personal data. The bank may then only store the data for the period of time required by law and can't perform any other processing operations on him;
- Alice does an online search using her name and surname. The results show a link to a newspaper article. The information in the newspaper dates back a number of years and is related to an issue about a real estate auction connected with debt recovery proceedings settled a long time ago and, therefore, nowadays irrelevant. If Alice is not a public figure and her interest in having the article removed outweighs the general public's interest in having access to the information then the search engine is obliged to remove links to web pages including her name and surname from the results.

5.1 Right to erasure

Under Article 17 of the GDPR individuals have the right to have personal data erased. This law is called the right to erasure or alternatively also known as the 'right to be forgotten'. The right to erasure is not a comprehensive law and only applies in specific situations. The rights of data subjects upon request to have their personal data erased includes the following scenarios : [Burri and Schär, 2016]

- The personal data is no longer necessary for the purpose it was originally collected or processed;
- The right to erasure relies on consent as lawful basis for holding the data, and the individual withdraws their consent;
- The right to erasure relies on legitimate interests as basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;
- The personal data is being processed for direct marketing purposes and the individual objects to that processing;
- The personal data is processed unlawfully (breach of the lawfulness requirement principle).

Special emphasis should be given to data collected from children if the data erased concerns minors who are under parental responsibility or guardian care. Particularly in online environments under the GDPR, this emphasis shows a realistic reflection and manifestation of the seriousness of enhanced protection of children data. [Burri and Schär, 2016]

If the data being processed is collected from children, particular leverage must be given for request from the data subject for erasure. This holds especially for processing of personal data on internet if the consent was given by a child data subject. Because a child data subject may not have been knowledgeable of the risks involved in the personal data processing at the time of consent, the right to erasure law still applies even if the data subject is no longer a child. [Burri and Schär, 2016]

If a processor or controller has revealed the personal data of a data subject to others, they must communicate with each and every recipient and notify the recipients about the

requested data erasure, unless doing so is determined to be impossible or involves excessive effort. If the data subject requests information about their personal data, the data subject has the right to know about the recipients who have access to the personal data of the data subjects. The GDPR defines controllers, processors and persons who are authorized to process personal data. They have access to recipients of the personal data who are natural or legal person, public authority, agency or other body to which the personal data are revealed. In an online public environment, appropriate measures should be considered to notify upon request to controllers processing personal data to erase links to, copies or replications of the personal data taking into account the cost of implementation and availing relevant technology. [Burri and Schär, 2016]

Ensuring the complete erasure of personal data from backup and live systems upon a legitimate request received from data subject should be executed based on the retention schedule and available technical means of the processor/controller. It is the responsibility of the controller/processor to notify the data subject as to what is going to happen to their data upon fulfilling their valid erasure request which includes both backup and live systems.[Burri and Schär, 2016]

There is a system in place to fulfil erasure request of the data subject from live systems but it is time consuming to get rid of the data backup systems. The important part of this procedure is that even if it is difficult to erase or overwrite the data immediately from backup system, the processor/controller should have a system in place to put the backup data hidden from public use.

Furthermore, the processor/controller should grant assurance that the data in the backup system is not utilized for any purpose. One of the ways to do this is that the processor/controller freezes the personal data or just merely retains in the system until it is replaced under a predetermined schedule. The erasure of personal data from backup system is is not a simple matter, e.g. retention poses a significant risk of unauthorized access to data from the backup while still it is not erased until a predetermined time. [Burri and Schär, 2016]

5.2 Secure data deletion

Secure data deletion means performing irreversible removal of data from a physical medium so that the original data is destroyed and can not be recovered by available technologies. Erasing data from the physical medium happens at different interfaces of layers which

adds complexity into the data deletion approach since the data is not securely erased by default in each layer. These interfaces of layers exist at user-level applications, at the file system, the device driver etc. Secure deletion of data at the different layers of interfaces requires different approaches which depend on the interface type. This secure data deletion procedure should be able to fulfil the task of deleting data from a physical medium so that the data is irrecoverable by any means. [Reardon et al., 2013]

Achieving secure data deletion of data by default in the digital world is presumably unattainable. However, there are different layers of actions that contribute to secure data deletion to existing physical medium interfaces. The different levels at which interfaces to the physical medium exist include user-level applications, the file system level, the device driver level etc. The properties of the approach differ significantly depending on which interface is in use. Avoiding the disclosure of sensitive data after disposal to physical medium is required as legislative or corporate stipulation especially concerning confidential communications. [Reardon et al., 2013]

Although all recent file systems enable users to "delete" their files from their system, which is in reality merely dissociating files indicating the file deletion, the actual contents still remain available since the meta data unlinking is ostensibly obscurely hiding the file. This method is contemplated to restore the resources dissipated instead of making the data inaccessible. The data, however, can be recovered by a technically knowledgeable user with low-level access to the storage system. In modern web browsers there is a privacy option known as clearing cache and web browsing history. Users apparently are tricked to believe that when they delete text messages and clear call logs from their phones, the deleted data is irrecoverable. [Reardon et al., 2013]

Among the numerous security strategies of secure data deletion is giving some form of access to an adversary on purpose as analogous to ethical hacking to ensure that there is no security vulnerability. This is done to test if that ambivalent intruder is not able to recover the data. For instance presumably one of the security strategies as a security purpose to achieve other goals is not disclosing session keys to an adversary in many key negotiations instead assigning tentative values thereby making session keys irretrievable. [Reardon et al., 2013]

5.3 Secure deletion by layers

As data is being stored extensively on electronic devices, achieving the privacy of sensitive information is utterly important and critical issue. Once the duration of storage is over, users are given the right to delete files from the storage system. However, the file deletion actually only modifies the meta data thereby retaining intact version of the data. The file still remains recoverable even after recreating the file system. This is the core reason why secure data deletion is introduced to completely wipe out the data from the storage system permanently.[Reardon et al., 2013]

Implementing secure data deletion at the higher layer interfaces will grant the lower level interfaces the functionality (see Figure 5.1). Special attention should be given to ensure that the secure data deletion mechanism is reliable. Some of the mechanisms are incapable resulting either in aggregate deletion of whole file from the physical medium or causing noticeable wear out. The figure illustrates the complexity of the data storage components in each layer and interface in physical medium, controller, device driver, file system and user applications interfaces.

The integral part of secure data deletion which is known as sanitizing the media, reliably and technically erases data from the physical medium. Media sanitization is a process by which data is irreversibly removed from media or the media is permanently destroyed. This mechanism ensures data integrity and confidentiality indirectly. Flash-based solid state disks (SSDs) have different internal architecture compared to hard drives which are well known in secure deletion of data from the entire disk as well as individual files.

[Reardon et al., 2013]

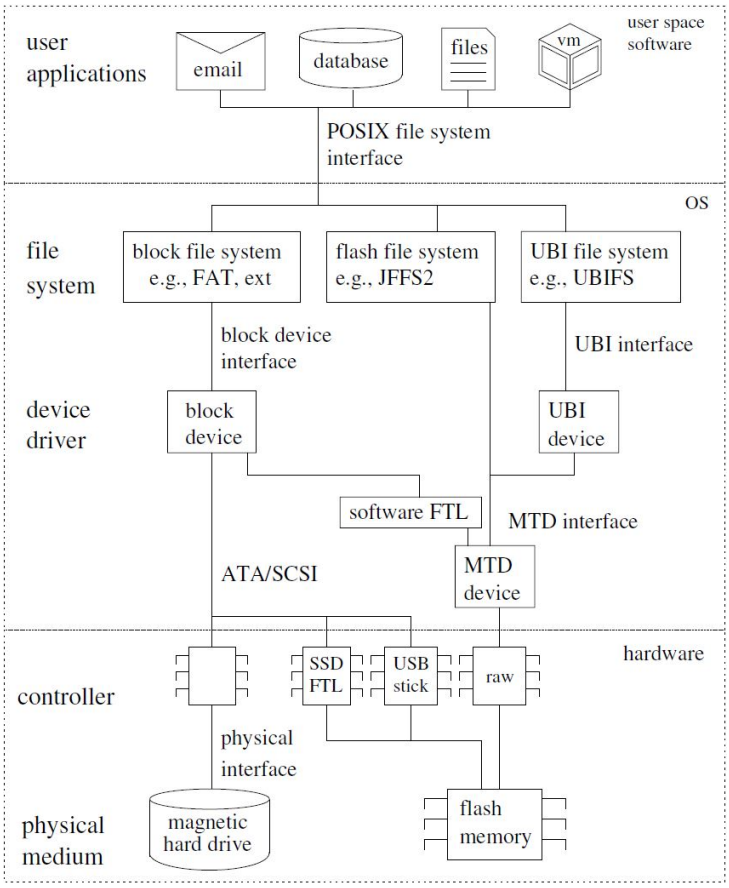

Figure 5.1: Some interfaces and layers involved in magnetic hard drive and flash memory data storage.[Reardon et al., 2013]

6 Block chain

Block chain is one of the major technological breakthroughs of the past decade. In order to build decentralized, trustworthy, inclusive, secure and egalitarian digital economy, block chain is recognized as a powerful instrument. Block chain enables transactions, reaching agreements and permanent record of information among large number of people and organizations. Block chain reformed the perception of the traditional central authority led economic, social and political institutions. [Berberich and Steiner, 2016]

Block chain derived its name from fundamental concept the technology is based on, which is data storage in clusters or groups known as blocks. Each authenticated block is cryptographically tied to the previous one. This forms incessant chain of data. There are numerous types of block chains currently, they all have basic operational attributes in common. The main functional characteristics all of the block chain versions share in common is providing a mechanism to enable direct communication of all nodes in the network. This communication is mainly in the form of transaction to add information to the database as well as a validation consensus in which the network can store the agreed version of the database. As the core idea of block chain technology is decentralization of the traditional central authority control, each node retains an identical replication of the block chain database and consistently update it as new valid blocks are added in the network.

Block chain is a technology nicknamed as the 'trust machine' for the attributes. This uniquely distinguishes it from the traditional approach of central authority approved transactions. Block chain allows large numbers of collaborators or competitors whether they are individuals or organizations to reach at consensus for storing information unalterably. [Berberich and Steiner, 2016]

6.1 Glossary of block chain

Below we will discuss the important terminology that is essential to understand the latest block chain technological advances as the vocabularies are quite specific.

the important terminology that is essential to understand the latest block chain techno-

logical advances.

6.1.1 Node

Node in the block chain network is merely a computer running the necessary software for processing information and communicating with the other nodes. All nodes keep identical copies of information in the block chain ledger.

6.1.2 Distributed ledger

A distributed ledger is a database that is consensually shared and synchronized across multiple sites, institutions, or geographies, accessible by multiple people. It allows transactions to have public "witnesses". The participant at each node of the network can access the recordings shared across that network and can own an identical copy of the recordings. Any changes or additions made to the ledger are reflected and copied to all participants in a matter of seconds or minutes.

A distributed ledger stands in contrast to a centralized ledger, which is the type of ledger that most companies use. A centralized ledger is more prone to cyber attacks and fraud, as it is a single point of failure.

6.1.3 Signature

A digital signature in public key cryptography is an authentication message to verify the authenticity and integrity of data communicated between sender and recipient nodes. The validity of the public key of the sender is guaranteed by a certificate granted by third party certification authorities. The integrity is still retained as the intruder is not able to alter the data without making the recipient to reject the digital signature. The digital signature ensures that the sender has actually the private key corresponding to the certified public key.

6.1.4 Transaction

The main technical information communication conducted through out a block chain network is the transaction where users behind every node send and receive the address, the value of transfer and data content exchanged. The digital signature message that every

user signs before sending the data using cryptographic private key enables nodes to control the validity of the signatures so that no intrusion has manipulated the data along its trajectory while traversing in the network. Digital signature is needed to ensure the origin of the data that is stored in the block chain.

6.1.5 Hash

Hash is similar to the digital version of a fingerprint, which is basically a function that utterly changes the actual data content into unique unintelligible format of constant length. It is not possible to produce the original data by reversing the hash function. This maintains security and reliability of the block chain network transaction.

6.1.6 Block

Block is the logical spot data structure in which the granular piece of information is stored or used to group transactions. Hash is computed over all data, including transactions, hash of the previous block and time stamp.

6.1.7 Smart contract

In block chain network, there are granular pieces of codes known as smart contracts stored in the network. Whenever they are deployed, smart contracts accomplish self execution automatically. These codes are important part of the block chain network that transform the business and services automation.

6.1.8 Token

Tokens are the digital versions of stocks, commodities and physical products that are considered as representation of assets securing and maintaining the block chain network.

6.1.9 Consensus algorithm

A consensus algorithm is a procedure through which all the peers of the block chain network reach a common agreement about the present state of the distributed ledger. In this way, consensus algorithms achieve reliability in the block chain network and establish

trust between unknown peers in a distributed computing environment. Essentially, the consensus protocol makes sure that every new block that is added to the block chain is the one and only version of the data that is agreed upon by all the nodes in the block chain.

The block chain consensus protocol consists of some specific objectives such as coming to an agreement, collaboration, co-operation, equal rights to every node and participation of each node in the consensus process. Thus, a consensus algorithm aims at finding a common agreement that is a win for the entire network.

The main advantage of consensus algorithm in the block chain network is the ability to control faulty or malicious actors. A single and immutable database ledger is recorded in the network and the filtering of bad actors achieved via different mechanisms.

The most famous consensus algorithms include *proof-of-work (PoW)*, *proof-of-stake (PoS)*, *proof-of-authority (PoA)*, *Proof of Burn (PoB)*, *Practical Byzantine Fault Tolerance (PBFT)*, *Proof of Capacity (PoC)* and *Proof of Elapsed Time (PoET)*. [Burri and Schär, 2016]

6.1.10 Validator nodes

Based on the consensus algorithm and following agreed upon rules, some specific nodes in the block chain are responsible in validating blocks and broadcasting them in the network. [Fabiano, 2017]

6.2 Interplay between block chain and the GDPR

The interplay between block chain and the GDPR is based on how the personal data is processed, the responsible pertinent body processing the personal information and analysis of the whereabouts the personal data surfaces or appears. Consortium of business entities and government agencies find applying and complying with the GDPR easier if they operate private, permissible block chain networks. The GDPR compliance interplay may be more difficult for public permissionless networks. The consortium using permissionless blockchain needs to be powerful enough to impose strict rules regarding personal data processing by defining the roles of participants, ensuring they follow terms and conditions set. Each consortium member is tied contractually to these terms and conditions. Contractual terms, for instance, includes monitoring the members not to view, and certainly not to utilize the personal data without permissions.

The 'privacy-by-design' compliance requirements of the GDPR can be easily fulfilled by private permissible networks of block chain application since monitoring the network is pretty achievable. However, when it comes to public permissionless block chains, GDPR compliance is relatively difficult to monitor due to the distributed nature of these network. Therefore, the next section will concentrate on analysis of the interplay between the GDPR and public, permissible block chain network introduced by Bitcoin. [Sullivan and Burger, 2017]

In principle, different versions of block chain network technology applications can abide by the requirements of the GDPR compliance. This is due to the fact that most block chain applications are operated by publicly identified known entity or consortium of entities. The entities manage the block chain database ledger on behalf of their users. These entities that operate the block chain application are data controllers that are mandated to fulfil the GDPR obligations. Technologists and entrepreneurs are concerned about whether the deployment of innovative applications on blockchain networks are compliant with GDPR requirements or not. However it is difficult to obtain a concrete answer to this question.

When it comes to the traditional client-server, or interchangeably known as client-provider network model, there is an identified controller whether it is a single entity or consortium of entities. The controller provides service or product that can be hold accountable and responsible for any infringements, regarding the purpose and means of collection and processing of personal data. [Neisse et al., 2017]

While in the traditional client/server model it is easy to identify the data controller, the main concern and object of debate in public permissionless block chain networks is to determine identity of a data controller. The fundamental idea behind this technology is collective processing of data via a peer-to-peer shared protocol. The answer to the identity of data controller in blockchain is not straightforward.

Open source technology projects in general, and open source block chain technology in particular, are desirable tools. The developers behind this useful technology should be appreciated and encouraged for such a commendable effort trying to make our daily life easier.

Holding these developers accountable for data collection and processing is analogous to holding Tim Berners-Lee accountable and responsible for everything that happened on the world wide web. These innovators and inventors are not to be hold accountable for the bad actors using their creative work irresponsibly as their intention is not providing such a commendable tool for infringement of data collection and processing. They rather deserve

compensation for the essence of their creativity rather than being held accountable for any violation the users cause.

The other debatable part of the block chain technology with respect to GDPR compliance is validating nodes we discussed earlier on as glossary of the block chain analysis section. These nodes or any other participating node in the block chain can not be considered as data controllers. The nodes that run the block chain technology protocol have different tasks but none of these tasks make them data controllers. One of the tasks is to validate other nodes. Another task is to participate in mining of new blocks in order to win a reward. The nodes also participate in distribution of transactions in peer to peer network and maintain a copy of the ledger, thus contributing to the stability of the block chain. Still another task of nodes is to access relevant data without relying on third party providers or intermediaries. They do not have the authority to determine the purpose and means of data collection and processing.

There are different cases that makes the accountability and responsibility of block chain more complex. The fact that even if it was possible to confront or approach physically the individuals who own the nodes and request them to edit or delete the data, it is extremely difficult for them to comply with the request. Even if they comply with the request and completely remove themselves from the network, the data is not deleted since every node has an immutable identical copy of the entire block chain database ledger.

The other GDPR compliance argument of block chain network is when and how individual nodes are considered to be data controllers. If the individuals behind nodes who sign and send transactions to the block chain database ledger submit personal data of others as part of their business activity which could be personal data of either those who are not part of the block chain or entities that operate block chain network software, products and services are to be considered most likely as data controllers. Sending personal data onto the block chain network no matter for whatever purpose this is done is not recommendable. However, if these node users send their own personal data so as to buy or sell crypto assets are exempted from being data controllers as household. [Albrecht, 2016]

The last point of debate about GDPR compliance of block chain technology is smart contracts. These granular pieces of software that are deployed to the block chain network can be independently executed solely by their publishers. Additionally whenever a network user call this software, the smart contracts are executed as well. The debate is about whether only the publisher, only the network user or both are to be the controllers.

6.3 Tensions between block chain and the GDPR

From the analysis we conducted above, there might be a temptation to conclude that block chain is not GDPR complaint due to the fact that a data controller can not be unequivocally determined despite the fact that data is processed but a data controller is not distinctly identified.

Although it seems at first glance that block chain contradicts inherently with GDPR, a more profound observations reveals that they share commonalities. The GDPR is based on the underlying assumption that in relation to each personal data there is atleast one natural or legal person. Block chains, however, often seek to achieve decentralisation in replacing a unitary actor with many different players. This makes the allocation of responsibility and accountability burdensome.

It is difficult to draw a sharp line and conclude as to whether block chain is GDPR compliant or not. Although this is serious concern, it does not mean that GDPR is going to determine the fate or the end of this tremendous technology let alone determining the fate of public permissible block chain networks. The courts, regulators or government agencies or the European Data Protection Board (EDPB) can not resolve the tension.

Regulatory agencies should gradually bring forth proposals that will clarify the issues of determining the identification and obligations of data controllers and processors, acknowledging that there are situations where it is difficult, and perhaps impossible, to identify data controllers. One example in this case is when individual users are posting transactions or calling decentralized smart contracts on a public, permissionless block chain for their own individual purpose. The proposal should focus on how to anonymize personal data, and the validity of various techniques that allow users to record 'proofs of data' on the block chain without actually revealing the data. Workplace data and information about education including salary, tax information and student numbers, private and subjective data including religion, political opinions and geo-tracking data should also be topic of concern in the proposal. The other issues the proposal should emphasize are lawfulness, data minimization, right to erasure and rectification, right of access, automated processing, territoriality and data protection by design and by default. [Wachter et al., 2017]

6.3.1 Points of conflicts

Despite the initial idea of the GDPR was to make it platform independent, data deletion and data editing, however, seem to contradict with the way the block chain network operates. The contrast is due to the inherent decentralization nature of block chain and presence of identical copy of the distribution ledger in each node makes it difficult editing and erasing data.

There are several key points where the block chain network technology does not abide by the GDPR mandates. These include fundamental features of the block chain such as block chain being decentralized and immutable, depends on a distributed ledger system that is permanent and that can not be interfered as well as not being controlled by any governing authority. [Lindqvist, 2017]

The personal details of data subjects can not be deleted or modified in the block chain network. If the block chain is used as a database transaction with personal information of data subjects, it will definitely contradict with GDPR mandates by default.

6.3.2 Block chain and decentralized ledger

One of the philosophies that fundamentally differentiates block chain and the GDPR is the data protection policy. Block chain strictly perceives about data protection and privacy rights being best preserved by advanced cryptography. This preservation strategy also includes immutable, permanent, decentralized and out of governing authority control distributed ledger system, storage and protection.

The regulators of the GDPR considered a centralized governing authority is vital to to protect consumers information from the abuses of private actors including the biggest data intensive technology tycoons such as FaceBook and Google. This characteristics of the centralized controller of data management fundamentally contradicts with the idea behind block chain. [Voigt and Von dem Bussche, 2017]

6.3.3 Data controller: nodes or nobody

The other feature that distinguishes GDPR and block chain is data controller roles. In case of block chain, the data controller roles set in the GDPR vanishes as a decentralized system has no one responsible and accountable for any discrepancies unlike the centralized

system where the roles are clearly marked on the actors of the system that can be easily identified. [Voigt and Von dem Bussche, 2017]

The intrinsically decentralized block chain system which uses a distributed ledger system enables any device or individual person behind a computer, known as node that runs the software, to join the peer-to-peer system. This peer-to-peer system maintains the network by preserving a replica of the block chain and the nodes have a copy of the distributed ledger. Nodes have no control or authority over the data in the network since they are part and parcel of a decentralized system. The nodes process data and once a node incorporates a block into the network, it is impossible to amend or rectify it as no one has control over data unlike a centralized system. [Salah et al., 2019]

There is argument that each and every node should be held responsible and accountable as they know what happens to their data and who accessed or shared their data using their private key. However nodes and data subjects actually, have limited control or no influence over the distributed ledger. Block chain storage system is decentralized therefore can not comply with GDPR mandates unlike the centralized system. [Neisse et al., 2017]

6.3.4 Immutability

As we discussed earlier the biggest conflict between block chain and GDPR mandates is the fact that data deletion and editing block chain are impossible. Deletion and editing of data are virtually impossible in block chain network. The right to be forgotten is one of the fundamental rights the GDPR stipulates. Data subjects upon request have the right that their personal information removed from whom stores their data. [Berryhill et al., 2018]

The right to be forgotten as the GDPR mandates is humorously converted to the right to be never forgotten in the case of block chain network since the data once incorporated in the immutable distributed ledger system can never be erased or amended in order to meet the GDPR requirements. Immutability and decentralization are the core ideas of the block chain network that stem from the fact that data security and integrity in the block chain preserves trustworthiness among nodes. [Mahankali, 2019]

Any alteration in the whole block chain network would compromise the entire system stems from the fact that blocks being comprised from subsequent blocks. The presence of a single corrupt block will damage the block chain system unless fixed swiftly since the block chain is updated by adding new transactions. [Zamani et al., 2018]

6.3.5 Coherences

The immutable nature of the block chain fundamentally reinforces integrity of data, improves the security and privacy of personal data governance, ensures transparency and provenance. This principle virtually coincides with GDPR objectives thereby makes block chain inherently compatible with GDPR. As we have been discussing block chain is strictly in conflict with GDPR mandates particularly with the right to be forgotten, deletion and modification of data subjects personal information. But a close observation reveals that both GDPR and block chain basically preserve security and privacy of data in two different approaches. [Lindqvist, 2017]

6.3.6 Individual control

Both the GDPR and block chain grant data subjects the freedom of control over their data although the degree of freedom of control in the case of block chain is restricted. Both GDPR and block chain apply the principle of data minimization. From the discussion we had in the whole section, it is conclusive that GDPR and block chain are contentiously conflicting and coherent at the same time.[Voigt and Von dem Bussche, 2017]

6.3.7 Anonymity

The fact that no personal information is revealed publicly even if a block chain is made public reinforces anonymity which is another shared commonality between GDPR and block chain. Allowing only participants transacting in the block chain network to view the other transacting participants' information and restricting other members on the network from viewing personal information of their peers preserves the core principle of anonymity. In case of permissioned public block chain the anonymity is preserved, since the private key is for allowing access and the public key is for indicating address in internal users' transactions, while these two purposes are detached from elements identifying personal information. [Hughes et al., 2019]

6.3.8 Transparency

Block chain uses encryption and decentralized structure to be profoundly resistant to tampering. This makes block chain hypothetically less vulnerable than a single instance

database system in case any unauthorized alteration tries to compromise the data integrity. Although encryption and decentralized distributed ledger system reinforces confidentiality and conceals clandestine information, all the transactions are entirely transparent and noticeably visible. [Berg et al., 2019]

6.3.9 Security

The key feature of block chain is the capability to store data across a variety of systems. The block chain guarantees the integrity of the data and prevents even breaches tampering single piece of data. Furthermore the decentralized transaction processing and the distributed ledger system completely avoids commonly exploited vulnerabilities that centralized data repositories are exposed to. [Zyskind et al., 2015]

6.3.10 Possible block chain solutions

There is a debate going around stakeholders on how to resolve the conflict between GDPR and block chain. Efforts to reconcile the conflict suggest mitigation in the operation of the block chain so that it can be inherently compliant with GDPR requirements. Block chain conflicts with GDPR rules making it illegal, future coexistence could be achieved by reforming fundamentally how the block chain functions. [Berryhill et al., 2018]

Off-chain storage

Segregating the data types stored on the block chain is one potentially viable solution to reconcile block chain with GDPR requirements. This means separately storing all personally identifiable information in “off-chain” databases and only referencing them with a hash of the data in the block chain. The references serve as control pointers to GDPR sensitive data. [Lindqvist, 2017]

Complete erasure of data in the off-chain storage database could be achieved by building protocols that serve for this purpose thereby obliging block chain to be GDPR requirements compliant. Therefore “right to be forgotten” could be exercised by data subjects, where the service provider completely erases the personal data upon request thereby removing “linkability” of the block chain hash pointer to the data located in distributed off-chain servers. This is a perfect solution making the referral information on the block chain useless without shutting down the entire block chain system. [Politou et al., 2019]

This solution, however, reduces the efficiency and effectiveness of the block chain retroactively reducing the capabilities of the block chain thereby affecting protection of personal data, security, integrity and transparency. [Politou et al., 2019]

Splitting data storage in block chain network platform exposes the information of data subjects and makes the system vulnerable to hacking and other intrusion attacks. This is because if personal data is stored in off-chain storage, the data subject has no means to know who has an authorized access to their data. This complexity results in vulnerability in the system, and makes development of global standards and deployment difficult. Adoption of block chain network for sensitive areas such as finance, supply chain and trade is a security risk especially with off-line storage. [Lindqvist, 2017]

Deletion of encryption keys

Keeping personal information on the block chain but at the same time making it inaccessible in case the data subject demands is an alternative solution adopted by some of the existing block chain companies. Erasure and revoking of personal information after certain interval upon request of the data subject makes the key that is used to encrypt the data unattainable thereby effectively erasing the key from the block chain network. [Mamo et al., 2020]

Throwing away encryption keys is not similar to 'erasure of data', which the GDPR underlines to be pursued as a strict rule. Therefore block chain does not comply with the GDPR requirements prohibiting storage of data in this case. Encrypted or hashed data is still considered as personal data under the GDPR since hashing or encryption of the personal data is merely pseudonymization of the data but not irreversible anonymization. [Voigt and Von dem Bussche, 2017]

6.4 Pseudonymization and anonymization

The combination of pseudonymization and off-chain data storage is an intriguing means to fulfill GDPR compliance. Under the GDPR a piece of data is said to be pseudonymous if and only if the data must "no longer be recognized as an attribute to a certain data subject unless otherwise additional information is required to re-identify a specific data subject." [Voigt and Von dem Bussche, 2017]

The right to erasure and the right to be forgotten with respect to the GDPR mandate

can be fulfilled using pseudonymization and off-chain storage scheme. This type of scheme enables the data subject to entirely remove their personal data. Links to off-chain data remain in the block chain but there is no data at the location where the link points to ("Error: no such file exists" ...) which means breaking the relation from the pointer to the data since the data is deleted. This is done by removing the any linkage to off-chain data from the system. [Teperdjian, 2020]

According to GDPR compliance, there are two conflicting interpretations with pseudonymization linkage to off-chain data storage in block chain. The first of the two contradictory interpretations is that GDPR compliance can be fulfilled since block chain hashing renders pseudonymization but not anonymization. Anonymization means the data linkage is deleted completely and re-identification of anonymous data is not possible. [Schwerin, 2018]

The second contradictory interpretation is based on the fact that tracing back to the original personal data is still possible despite using pseudonymization with cryptographic hashes. Pseudonymization makes it extremely challenging for users to identify data, but it does not completely remove the original data and still allows re-identification of the personal information stored in off-chain. [Bolognini and Bistolfi, 2017]

Overall, in order for data to be considered pseudonymous under GDPR, the data must "no longer be attributed to a specific data subject without the use of additional information". Pseudonymization with pointers to personal data stored off-chain in a manner which allows the personal data to be destroyed and thus removes the link to the data on the chain and renders it anonymized may allow a user to remove all of their personal information from the chain, as required by the GDPR's right to erasure.

Self-sovereign identity (Sovrin) application

One of the means for individuals also known as data subjects for protecting their personal data is controlling and monitoring their digital identities using block chain network technology compliant with GDPR rules. One protocol that enables individuals to control and monitor their personal information is known as Sovrin. The Sovrin ledger database application does not actually store the personal data of individuals known as data subjects. Instead it serves as a directory of pointers to the personal data of individuals that are stored in traditional centralized database systems. Sovrin takes extra security measures to fulfil the GDPR's "privacy by design and default" principles. [Onik et al., 2019]

In the block chain regime, nodes are also known as peers and they are data subjects,

individuals who own personal data. These peers grant limited access to third parties and provide information to other peers that is necessary for a specific business transaction and purpose. In-order to be GDPR compliant whoever accessed the data leaves traces in the block chain ledger. This means block chain ledger contains an immutable record of entities who accessed the data and how they are using the data registered perpetually. [Miyachi and Mackey, 2021]

Use of private or enterprise block chains

Block chain systems used inside a single company is one way to achieve GDPR compliance since in that case the block chain can be private. Instead of just one company, several companies may share a private block chain. The block chain could be permissionless or permissioned. These private and enterprise block chains are not similar to public block chains which grant access to unlimited number of users. Both private and public block chains are based on decentralized utility. The private and enterprise block chains restrict the dissemination of personl data of individuals or data subjects to a limited number of entities or just to one entity. Consequently the size of the block chain is reduced and thereby the spread of sensitive information as well as the amount of data breaches is minimized. [Casino et al., 2019]

Centralized back-end system

The best solution to bypass or circumvent the GDPR non-compliance of block chain network technology is to implement a centralized back-end system. However, this fundamentally changes how the block chain operates. This method would help in anonymization of the data without damaging any chains in the network. The problem with this concept is that it utterly alters the way the block chain network is built and meant to function. [Voigt and Von dem Bussche, 2017]

6.5 Block chain and regulators

By the time the GDPR was still on planning phase in European Commission, the block chain technology was already emerging. When the regulation got implemented, the block chain was an established technology which got affected by the new rules of GDPR. [Corrales et al., 2019]

From the preceding explanatory deliberations about the GDPR and block chain, one can deduce that block chain is a technology that is fundamentally built to be incompatible

to the GDPR compliance. The problem with the GDPR is that it does not take into consideration the existence of inherently decentralized, distributed system of the block chain. The block chain is not under the control and monitoring of central authority. The difficult challenge is how to proceed to make GDPR compliant block chain system. On the other hand, the regulators should consider means of leaving the full potential of the block chain intact. [Politou et al., 2019]

The preliminary responsibility and initiative should come from the GDPR regulators and European commission authorities to take steps to reform the rules. The rules need to be inclusive of the block chain adding flexibility and clarity to the regulation. The making of inclusive rule should recognize the fact that block chain is built on a decentralized distributed system and consider mechanisms to support the block chain by enhancing data privacy and protection as well as prevention of data breaches. [Keller, 2018]

6.5.1 Rigid GDPR approach

Before the GDPR regulators can take legal enforcement actions, there is a need for clarifications and removal of uncertainties revolving around GDPR compliance. A gray area exists in GDPR principles definition and interpretation. Therefore exhaustive implementation is required to resolve the issue. [Teperdjian, 2020]

The legal enforcement loophole is particularly reflected in public block chains. The European commission regulators are not in a position to maintain strict legal enforcement into action when it comes to public block chains. Courts can not even file charges as there is no one responsible pertinent body to document and print their name on the court document. This is merely accusing all users in the block chain network for any irregularity or trespassing. It may be easier to find a responsible entity in private block chain. [Hoofnagle et al., 2019]

6.5.2 Self-regulation

Short term solution to the GDPR incompatibility and non-compliance with the block chain could be requiring self regulation from block chain technology. This means letting the block chain network technology to come up with a mechanism to preserve personal data privacy and protecting against data breaches. One consequence is that block chain start-ups should collect less data points. This is the better way to restrict personal data exposure

than using hashes instead of other personal data such as identifiers. [Ahmed et al., 2020]

6.5.3 Create legal certainty and clarity

One of the responsibilities of the GDPR regulators is making sure that the legislation is clear. The legislation should provide explanatory elaboration on definitions and interpretations of the rules such as the right to be forgotten and its enforcement, as well as how to handle personal data. For instance, the GDPR's definition of personal data is generic and might refer to anything that can be traced back to an identifiable physical person. This could be, for instance, name, IP address, unique public key as well as address on the block chain. We can infer that personal data is one part of the GDPR regulatory grey area. [De Hert and Papakonstantinou, 2012]

Another illusion and confusion that follows from GDPR lacking clarity is the definition and interpretation of the right to be forgotten or "erasure of data". The data portability and rectification rules are not concretely defined either. The definition falls short in clarifying what erasure of data really means. Some questions are whether a person could really be forgotten and what physical or logical deletion actually imply in terms of permanently making the data anonymous. The comparison is between having no means to trace back the block chain to a specific user and data exchange versus truly forgetting the data subject, the individual to whom the personal data belongs to. The lack of clarity in the definition can lead to a conclusion that "erasure" does not mean that data is merely deleted and that making data perpetually inaccessible without deletion should yield the same result and be considered as deletion of data. [Hoofnagle et al., 2019]

There still remains a tone of unanswered questions concerning the block chain network technology and GDPR compliance. One of the unanswered questions is the following controllers get penalized if they do not delete "their own copy" of data but they do not get fines when they are not able to delete"public" copies for reasons of technology and costs. [Hoofnagle et al., 2019]

6.5.4 Regulatory flexibility: balanced approach

GDPR regulators need to be flexible with block chain and other innovative developments. They should acknowledge the inherently important features these technologies are established on. These features include immutability, centralized structures and lack of central

authority that serves as central data controller. Except the lack of a responsible and accountable data controller in block chain, the other feature indeed promote data privacy protection and security preventing against data breaches. As a result regulators need to balance between the objectives of these abundantly emerging innovative developments on one hand and the personal data privacy protection which is the core of the GDPR on the other hand. [Andoni et al., 2019]

Whether public keys are personal data and what type of substantive rights need to be granted regarding the nature of the data controller in case of block chain requires favourable interpretation and flexibility by EU regulators. [Andoni et al., 2019]

A convenient way forward could be creating a framework of governance in which innovative technologies reveal all stored personal data on-chain and off-chain and manage these data responsibly. Regulators on the other side should be implementing rules that encourage and realize the benefits of these technologies and regulate the rules to minimize the harms inflicted by these abundantly emerging technologies and prevent against data breach. [Reijers et al., 2018]

6.5.5 Cooperative approach: Dialogue

In the rest of this section, different approaches and viewpoints are discussed which would help in reducing the incompatibility between GDPR and block chain technology. The EU regulators should be aware of the reality that decentralized platforms such as block chains are ubiquitous and the only way forward is deliberation and mutual consensus among stakeholders. The fate of data protection and privacy depends on dialogue and common understanding among all stakeholders including regulators, innovators and the technology industry in general. The future block chains are in all shapes and forms influenced by the decisions made today by all pertinent bodies. The decisions can be helpful for the society especially respecting data privacy. [Berg et al., 2019]

There should be a cooperative approach, blend of transparent transactions, privacy controls and freedom of building useful innovations, a common understanding and mutual consensus that should be commonly shared among regulators, policy makers, innovators and users. Regulators should play a decisive role encouraging developers in various ways such as providing incentives to build platforms that respect the fundamental rights of people. Regulators should also guide developers on how to build GDPR compliant systems. [De Hert and Papakonstantinou, 2012]

6.5.6 Amending GDPR rules

Deliberations among stakeholders of the GDPR should bring appropriate amendments in the existing GDPR rules. Regulators should appreciate and encourage the fundamental unique characteristics and specifics of the block chain and other innovative technologies. Various amendments should for instance ascertain that the right to be forgotten is accommodated and incorporated in block chain network and other similar technologies. [Schwerin, 2018]

6.5.7 Forward thinking

The way forward should be based on practical instead of dogmatic approach by the GDPR. As long-lasting uncertainties around the GDPR could impede the progress of block chain and discourage the emergence of other similar innovative technologies. Clarity should be given by regulators on the future approach that is essential for the fate of the block chain network technology and other similar innovations. [Keller, 2018]

Intermediary compromise approach need to be prevented as it may affect the fundamental unique characteristics and specifics of the block chain technology and the benefits harvested from it. The potential combination of the distributed ledger and GDPR will improve the way companies collect, store, process and utilize personal data and private information. This can be used to build trust and transparency among entities reinforcing data ownership. [Politou et al., 2019]

7 Conclusion

The GDPR emphasizes the importance of data security and privacy. Over 20 years span the directive that was effective before GDPR gave prominence for security but did not cover data privacy. Data breach, unauthorized or unlawful processing, accidental harm to personal data and destruction of personal data are among the many scenarios security is concerned with. The legislation is formulated to help protect the rights of individuals predominantly. On the other hand, it arguably imposes massive responsibility on data controllers and data processors.

The GDPR rights for individuals include the right to be informed, the right of access, the right to rectification, the right to erasure, the right to restrict processing, the right to data portability, the right to object and also rights around automated decision making and profiling. In all of these cases security and privacy of personal data is the primary concern.

One of the most contentious elements of the GDPR is the capability and privilege granted for regulators to punish, with huge fines, businesses who do not comply with GDPR requirements. An organization that does not handle and process an individual's data in the proper and correct way can be fined. If an organization does not have a data protection officer when GDPR requires it, the organization can be fined as well.

Block chain is a promising new technology for many different purposes. At first glance GDPR and block chain seem to contradict each other, but actually they have many common principles. There are aspects where the block chain and the GDPR are in line with each other. Both block chain and GDPR nurture transparency, enhance individual rights as well as privacy and security of personal data. These are the core features in handling personal data which benefit data subjects.

The main conflicting feature between GDPR and block chain is the right to be forgotten. The GDPR grants individuals the privilege to erase their data from a public record while block chain block chain cannot do that because it is inherently immutable. Data could be deleted also in the case of block chain but typically there is a pointer that will indicate where the data is stored.

One of the main differences between the two concepts is that block chain is immutable

while the GDPR gives users the right to add, delete, modify and erase their personal information from public records. Another difference stems from the fact that block chain is a decentralized distributed ledger system where there is no monitoring central authority, and there is no distinction between data processors and data controllers. The GDPR implies a centralized system controlled by a monitoring authority. Still another difference is that GDPR covers cases where identities of users or data subjects are known whereas block chain deals with anonymous users. More constructive work should be made to bring block chain to GDPR compliance.

References

[Absalom, 2012] Absalom, R. (2012). International data privacy legislation review: A guide for byod policies. *Ovum Consulting, IT006*, 234:3–5.

[Ahmed et al., 2020] Ahmed, J., Yildirim, S., Nowostaki, M., Ramachandra, R., Elezaj, O., and Abomohara, M. (2020). Gdpr compliant consent driven data protection in online social networks: A blockchain-based approach. In *2020 3rd International Conference on Information and Computer Technologies (ICICT)*, pages 307–312. IEEE.

[Albrecht, 2016] Albrecht, J. P. (2016). How the GDPR will change the world. *Eur. Data Prot. L. Rev.*, 2:287.

[Amin et al., 2004] Amin, R. B., Hanley, D. V., Morrow, G. C., and Allahyari, J. (2004). Architecture for an IP centric distributed network. US Patent 6,714,987.

[Andoni et al., 2019] Andoni, M., Robu, V., Flynn, D., Abram, S., Geach, D., Jenkins, D., McCallum, P., and Peacock, A. (2019). Blockchain technology in the energy sector: A systematic review of challenges and opportunities. *Renewable and Sustainable Energy Reviews*, 100:143–174.

[Berberich and Steiner, 2016] Berberich, M. and Steiner, M. (2016). Blockchain technology and the GDPR-how to reconcile privacy and distributed ledgers. *Eur. Data Prot. L. Rev.*, 2:422.

[Berg et al., 2019] Berg, C., Davidson, S., and Potts, J. (2019). *Understanding the blockchain economy: An introduction to institutional cryptoeconomics*. Edward Elgar Publishing.

[Berryhill et al., 2018] Berryhill, J., Bourgery, T., and Hanson, A. (2018). Blockchains unchained: Blockchain technology and its use in the public sector.

[Bolognini and Bistolfi, 2017] Bolognini, L. and Bistolfi, C. (2017). Pseudonymization and impacts of big (personal/anonymous) data processing in the transition from the directive 95/46/ec to the new eu general data protection regulation. *Computer Law & Security Review*, 33(2):171–181.

[Burri and Schär, 2016] Burri, M. and Schär, R. (2016). The reform of the EU data protection framework: outlining key changes and assessing their fitness for a data-driven economy. *Journal of Information Policy*, 6(1):479–511.

[Calder, 2016] Calder, A. (2016). *EU GDPR A Pocket Guide*. IT Governance Ltd.

[Casino et al., 2019] Casino, F., Dasaklis, T. K., and Patsakis, C. (2019). A systematic literature review of blockchain-based applications: current status, classification and open issues. *Telematics and informatics*, 36:55–81.

[Corrales et al., 2019] Corrales, M., Jurčys, P., and Kousiouris, G. (2019). Smart contracts and smart disclosure: coding a gdpr compliance framework. In *Legal Tech, Smart Contracts and Blockchain*, pages 189–220. Springer.

[De Hert and Papakonstantinou, 2012] De Hert, P. and Papakonstantinou, V. (2012). The proposed data protection regulation replacing directive 95/46/ec: A sound system for the protection of individuals. *Computer law & security review*, 28(2):130–142.

[Diker Vanberg and Ünver, 2017] Diker Vanberg, A. and Ünver, M. B. (2017). The right to data portability in the gdpr and eu competition law: odd couple or dynamic duo? *European Journal of Law and Technology*, 8(1).

[Dzikegielewska, 2017] Dzikegielewska, O. (2017). Anonymization, tokenization, encryption: how to recover unrecoverable data. *Computer Science and Mathematical Modelling*, 6(4):9–13.

[Fabiano, 2017] Fabiano, N. (2017). The internet of things ecosystem: The blockchain and privacy issues. the challenge for a global privacy standard. In *2017 International Conference on Internet of Things for the Global Community (IoTGC)*, pages 1–7. IEEE.

[Finseth et al., 1993] Finseth, C. et al. (1993). An access control protocol, sometimes called tacacs. Technical report, RFC 1492, July.

[Gilbert, 2011] Gilbert, F. (2011). European data protection 2.0: new compliance requirements in sight-what the proposed EU data protection regulation means for us companies. *Santa Clara Computer & High Tech. LJ*, 28:815.

[GROOT, 2017] GROOT, J. D. (2017). What is the General Data Protection Regulation? understanding complying with GDPR requirements in 2019. *https://digitalguardian.com/blog/what-gdpr-general-data-protection-regulation-understanding-and-complying-gdpr-data-protection. Accessed*, 1.

[Gupta et al., 2001] Gupta, A., Kleinberg, J., Kumar, A., Rastogi, R., and Yener, B. (2001). Provisioning a virtual private network: a network design problem for multicommodity flow. In *Proceedings of the thirty-third annual ACM symposium on Theory of computing*, pages 389–398. ACM.

[Hoofnagle et al., 2019] Hoofnagle, C. J., van der Sloot, B., and Borgesius, F. Z. (2019). The european union general data protection regulation: what it is and what it means. *Information & Communications Technology Law*, 28(1):65–98.

[Hughes et al., 2019] Hughes, L., Dwivedi, Y. K., Misra, S. K., Rana, N. P., Raghavan, V., and Akella, V. (2019). Blockchain research, practice and policy: Applications, benefits, limitations, emerging research themes and research agenda. *International Journal of Information Management*, 49:114–129.

[Keller, 2018] Keller, D. (2018). The right tools: Europe's intermediary liability laws and the eu 2016 general data protection regulation. *Berkeley Tech. LJ*, 33:287.

[Kennedy and Millard, 2016] Kennedy, E. and Millard, C. (2016). Data security and multi-factor authentication: Analysis of requirements under EU law and in selected EU member states. *Computer Law & Security Review*, 32(1):91–110.

[Koops, 2014] Koops, B.-J. (2014). The trouble with European data protection law. *International Data Privacy Law*, 4(4):250–261.

[Kuner, 2012] Kuner, C. (2012). The european commission's proposed data protection regulation: A copernican revolution in european data protection law. *Bloomberg BNA Privacy and Security Law Report (2012) February*, 6(2012):1–15.

[Lambert, 2016] Lambert, P. (2016). *The Data Protection Officer: Profession, Rules, and Role*. CRC Press.

[Lindqvist, 2017] Lindqvist, J. (2017). New challenges to personal data processing agreements: is the GDPR fit to deal with contract, accountability and liability in a world of the internet of things? *International Journal of Law and Information Technology*, 26(1):45–63.

[Mahankali, 2019] Mahankali, S. (2019). *Blockchain: The Untold Story: From birth of Internet to future of Blockchain*. BPB Publications.

[Mamo et al., 2020] Mamo, N., Martin, G. M., Desira, M., Ellul, B., and Ebejer, J.-P. (2020). Dwarna: a blockchain solution for dynamic consent in biobanking. *European Journal of Human Genetics*, 28(5):609–626.

[McCall, 2018] McCall, B. (2018). What does the GDPR mean for the medical community? *The Lancet*, 391(10127):1249–1250.

[McDowell, 2019] McDowell, B. (2019). Three ways in which GDPR impacts authentication. *Computer Fraud & Security*, 2019(2):9–12.

[Miyachi and Mackey, 2021] Miyachi, K. and Mackey, T. K. (2021). hocbs: A privacy-preserving blockchain framework for healthcare data leveraging an on-chain and off-chain system design. *Information Processing & Management*, 58(3):102535.

[Neisse et al., 2017] Neisse, R., Steri, G., and Nai-Fovino, I. (2017). A blockchain-based approach for data accountability and provenance tracking. In *Proceedings of the 12th International Conference on Availability, Reliability and Security*, pages 1–10.

[Nelson, 2011] Nelson, D. (2011). Crypto-agility requirements for remote authentication dial-in user service (radius). Technical report, RFC 6421, November.

[Nyrén et al., 2014] Nyrén, O., Stenbeck, M., and Grönberg, H. (2014). The european parliament proposal for the new EU general data protection regulation may severely restrict European epidemiological research. *European journal of epidemiology*, 29(4):227–230.

[Onik et al., 2019] Onik, M. M. H., Kim, C.-S., Lee, N.-Y., and Yang, J. (2019). Privacy-aware blockchain for personal data sharing and tracking. *Open Computer Science*, 9(1):80–91.

[Politou et al., 2018] Politou, E., Alepis, E., and Patsakis, C. (2018). Forgetting personal data and revoking consent under the gdpr: Challenges and proposed solutions. *Journal of Cybersecurity*, 4(1):tyy001.

[Politou et al., 2019] Politou, E., Casino, F., Alepis, E., and Patsakis, C. (2019). Blockchain mutability: Challenges and proposed solutions. *IEEE Transactions on Emerging Topics in Computing*.

[Purtova, 2018] Purtova, N. (2018). The law of everything. broad concept of personal data and future of eu data protection law. *Law, Innovation and Technology*, 10(1):40–81.

[Reardon et al., 2013] Reardon, J., Basin, D., and Capkun, S. (2013). Sok: Secure data deletion. In *2013 IEEE Symposium on Security and Privacy*, pages 301–315. IEEE.

[Reijers et al., 2018] Reijers, W., Wuisman, I., Mannan, M., De Filippi, P., Wray, C., Rae-Looi, V., Vélez, A. C., and Orgad, L. (2018). Now the code runs itself: On-chain and off-chain governance of blockchain technologies. *Topoi*, pages 1–11.

[Salah et al., 2019] Salah, K., Rehman, M. H. U., Nizamuddin, N., and Al-Fuqaha, A. (2019). Blockchain for ai: Review and open research challenges. *IEEE Access*, 7:10127–10149.

[Schwerin, 2018] Schwerin, S. (2018). Blockchain and privacy protection in the case of the european general data protection regulation (gdpr): a delphi study. *The Journal of the British Blockchain Association*, 1(1):3554.

[Spindler and Schmechel, 2016] Spindler, G. and Schmechel, P. (2016). Personal data and encryption in the european general data protection regulation. *J. Intell. Prop. Info. Tech. & Elec. Com. L.*, 7:163.

[Sullivan and Burger, 2017] Sullivan, C. and Burger, E. (2017). E-residency and blockchain. *computer law & security review*, 33(4):470–481.

[Tankard, 2016] Tankard, C. (2016). What the GDPR means for businesses. *Network Security*, 2016(6):5–8.

[Teperdjian, 2020] Teperdjian, R. (2020). The puzzle of squaring blockchain with the general data protection regulation. *Jurimetrics Journal*.

[Tikkinen-Piri et al., 2018] Tikkinen-Piri, C., Rohunen, A., and Markkula, J. (2018). EU general data protection regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review*, 34(1):134–153.

[Vandenbroucke and Olsen, 2013] Vandenbroucke, J. P. and Olsen, J. (2013). Informed consent and the new EU regulation on data protection. *International journal of epidemiology*, 42(6):1891–1892.

[Voigt and Von dem Bussche, 2017] Voigt, P. and Von dem Bussche, A. (2017). The EU general data protection regulation (gdpr). *A Practical Guide, 1st Ed., Cham: Springer International Publishing*.

[Voss, 2017] Voss, W. G. (2017). European union data privacy law reform: General data protection regulation, privacy shield, and the right to delisting. *The Business Lawyer*, pages 76–99.

[Wachter et al., 2017] Wachter, S., Mittelstadt, B., and Floridi, L. (2017). Why a right to explanation of automated decision-making does not exist in the general data protection regulation. *International Data Privacy Law*, 7(2):76–99.

[Weir et al., 2017] Weir, G., Aßmuth, A., Whittington, M., and Duncan, B. (2017). Cloud accounting systems, the audit trail, forensics and the EU GDPR: how hard can it be? In *British Accounting & Finance Association (BAFA) Annual Conference 2017*.

[Zamani et al., 2018] Zamani, M., Movahedi, M., and Raykova, M. (2018). Rapidchain: Scaling blockchain via full sharding. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, pages 931–948.

[Zyskind et al., 2015] Zyskind, G., Nathan, O., et al. (2015). Decentralizing privacy: Using blockchain to protect personal data. In *2015 IEEE Security and Privacy Workshops*, pages 180–184. IEEE.