RIGA GRADUATE SCHOOL OF LAW

Electronic identity verification: personal data protection challenges and risks

MASTER'S THESIS

Author: Elvīra Krēķe
LL.M. 2018/2019-year student
student number B018036

SUPERVISOR Dr. iur. IRĒNA ĶESTEROVA

DECLARATION OF HONOUR:

I declare that this thesis is my own work, and that all references to, or quotations from, the work of others are fully and correctly cited

.....

RIGA, 2020

Abstract

This work highlights the clash of GDPR, eIDAS Regulation and PSD2 Directive, as well as tackles challenges of implementation in practice, specifically the challenges of securing personal data whilst ensuring an electronic identity. A comparative analysis on practical case studies which are concerned with electronic identity verification, electronic identity establishment and use electronic identity verification in the process of providing services is carried out in order to understand how such businesses tackle personal data challenges, how successfully and to what manner. The work concludes with findings of legal uncertainty between all three regulatory acts, as they lack unified definitions and interpretational certainty in terminology, as well as they are in a need of revision due to the fact that some relevant laws were developed prior GDPR.

Summary

This research tackles to find possible overlaps and challenges in balancing the principle of retaining control over personal data and online identity amongst three regulatory acts – the General data protection regulation eIDAS, and PSD2.

The topic for Master thesis was chosen due to its relevance, namely due to the fact that until the end of 2020, all payment service providers and companies based in the EU must implement PSD2 Strong Customer Authentication, as well as, the incentive for PSD2 to strive for open banking, and eIDAS which establishes a definition and rules for trust services, online identity and deals with user authentication - all have raised many discussions on personal data privacy, control over personal data, security and how they interact with GDPR. For data protection enthusiasts, the incentive to establish access to personal data and the creation of online identities means going against the purpose of ensuring online privacy, control over personal data and online anonymity. The clear clash of both incentives is apparent, therefore it was chosen to be looked at in more detail throughout this work.

The first part of the research explains the fundamentals of EU personal data protection – history, legal framework of data protection and highlights the topicality of personal data protection. The topicality of the issue is highlighted by providing with information on why personal data are at such high value, in what malicious ways personal data can be used and therefore why personal data, specifically, identities must be protected. Additionally, the first part provides with an introduction to electronic verification in the light of GDPR and tackles Article 15 of the GDPR and its "Right of access by the data subject" where the necessity to identify one's identity in a proper manner emerges.

The second part of the work provides with an in-depth explanation on electronic identity verification schemes, services and electronic identities are provided, along with the legal framework and technicality of such schemes, in order to understand the possible points of clash. The second part introduces eIDAS, PSD2 and the 4th AMLD in regards to electronis identification, explains the authentication levels of assurance and distinguishes trust services from e-services and how they interact with GDPR.

Furthermore, the second part carries out case studies on 4 legal entities which are concerned with electronic identity verification, electronic identity establishment or use electronic identity verification in their operational work, are carried out in order to see how they implement GDPR principles, are they compliant and whether they ensure the highest level of security, as well as how far can such businesses strive for and ensure online anonymity and if it is possible. Furthermore, a comparison between certain principles of regulatory acts is made in order to understand the key differences in why the compliance to all three regulatory acts may be challenging.

During the research, analytical research was carried out on four service providers: 1) SmartID, which is a trust service provider ensuring an identity verification tool; 2) Dokobit, an electronic service which provides with the opportunity to sign documents electronically; 3) Veriff, a third party identity verification tool, which differs from SmartID with the fact that it is not a qualified trust service provider and provides with KYC solutions worldwide, and lastly 4) Gov.UK Verify, which is a UK eGovernment eID scheme, allowing to verify an individual's identity by various means before using eGovernment services. Case studies show that while all service providers claim to be GDPR compliant, all face compliance challenges, either regulatory or technical, and some raise questions of potential risks.

The research concludes with findings that all three regulatory acts pose challenges where the scope of the definition of certain terminology does not align, as for instance, in PSD2 and GDPR the term and conditions for 'consent' differ, moreover, the term 'pseudonymisation' is to be understood differently between GDPR and eIDAS. Apart from interpretational challenges, it is not clear on which regulatory act prevails, therefore it is looked at whether PSD2 could be considered as *lex specialis* in regards to GDPR and concludes that eIDAS does not share the same terminology due to the fact that it was developed prior GDPR. Lastly, the work carries out a comparison between case studies and gives proposals to how ensure the highest level of data privacy, data protection and potentially overcome the posed regulatory challenges in order to ensure the highest level of personal data protection.

Table of Contents

1. Fundamentals of personal data protection 8
1.1. The value of personal data 9
1.2. Personal data related crimes: identity theft 10
1.3. The emergence and role of the GDPR 12
1.3.1. General concepts of data protection 15
1.3.2. Legal grounds for processing data 16
1.3.3. Data subject rights 17
1.3.4. Art. 15 Right of access by the data subject 18
2. Online Identity and eID verification 21
2.1. eIDAS, PSD2 and 4th Amendment of the AMLD 22
2.2. Authentication levels of assurance 24
2.3. Trust Services, E-services and GDPR 26
2.3.1. Case Study: SmartID in the Baltics 27
2.3.2. Case Study: Dokobit 28
2.4. Electronic identity verification and third party providers 30
2.4.1. Case Study: Gov.UK Verify 31
2.4.2. Case Study: Veriff 32
3. Comparative analysis on GDPR, eIDAS and PSD2. 34
3.1. Comparative analysis on case studies 34
3.2. The clash of eIDAS, PSD2 and GDPR 37
3.2.1. Open banking vs. GDPR 37
3.2.2. eIDAS vs. GDPR 39
4. Conclusion 44

Introduction

Due to rapidly evolving technologies, digital trends, specifically striving for receiving services, especially financial services remotely, the topic of electronic identity verification and electronic identity has become widely topical. However, the creation of online electronic identity holds vast amount of personal data, including biometrical data, which raises concerns in regards to personal data protection and privacy. eIDAS Regulation and the new PSD2 Directive strive for establishment of an electronic identity, regulate electronic identity verification, trust service providers, as well as impose obligations to comply with secure authentication in order to preclude the technological development in line with the regulatory acts, however, it must be weighed whether it does not pose risks to personal data protection, and how both regulatory acts interact with GDPR and the principles therein.

Research question – Does one of the main aims of GDPR to ensure data subject control over personal data conflict with eIDAS Regulation and PSD2 Directive to ensure electronic identification and establish an online identity?

Hypothesis - GDPR's main aim to provide data subjects with more control over personal data and protect the personal data clashes with the eIDAS and PSD2 aim to establish online identity and access to data due to legal uncertainty between the interaction of the three regulatory acts and the terminology therein.

Structure and Scope

This work is constructed in a way to emphasize the online realm of electronic identities and personal data protection law, how they interact and whether they do not clash by carrying out a comparative research between practical application of data protection laws and a comparative research between the relevant regulatory acts, namely PSD2 Directive, eIDAS Regulation and GDPR.

The first part of the work underlines the importance of data protection, as well as explains the fundamental concepts of data protection, followed by the second part, which describes what is an electronic identity, how an electronic identity can be established and how it can be verified. Relevant regulatory acts are introduced in the second part as well, followed by four case studies on enterprises which are concerned with electronic identity verification or use electronic verification in their day-to-day operations and how relevant data protection laws are complied with.

This research is carried out from a perspective where ensuring online anonymity is the best case scenario, however, understanding that anonymous data are not in the scope of GDPR, the case studies are carried out in a manner of analyzing whether all service providers have ensured the maximum data protection taken into account all the available technical means.

Finally, the last part of the work carries out an analysis of the research done beforehand and draws conclusions on the challenges that all three regulatory acts face and comes to a conclusion that regulatory acts must be subjected to secondary revision after the introduction of GDPR, due to legal certainty arising out of inconsistent terminology and concepts therein. As the concepts which possibly clash are many, one is chosen for each regulatory act, namely, during the comparative analysis between PSD2 and GDPR, the term

'consent' is to be compared. In contrast, in the process of comparing eIDAS and GDPR, the definition of 'pseudoymisiation' is tackled.

The research concludes with findings of legal uncertainty and clashes of terminology amongst all regulatory acts, possible data breach risks in case studies and gives proposals to solve the aforementioned concerning issues.

Methodology

Due to the comparison and the use of the aforementioned regulatory acts used for the analysis, the research mostly encompasses the use of doctrinal method by taking GDPR, eIDAS and PSD2 as the fundamental source for this research. During the case studies, analytical research was carried out by accessing the respective services and analyzing on how certain GDPR principles have been applied in practice. Many research was used to support the findings in the process of the analysis. Furthermore, the key differences and clash between the interpretation of certain terminology in all three regulatory acts was carried out by using comparative method, by comparing how all three acts interact and the findings were supported by similar research carried out on this particular topic as well.

Legal Study

This work is carried out in the field of personal data protection, which looks at personal data protection challenges, implementation and the interaction between the online realm of electronic identities. In order to carry out a successful comparative research, the fundamentals of data protection need to be tackled, followed by a description of what is an electronic identity, how an electronic identity can be verified, the relevant acts and practical case studies on how such businesses ensure data privacy. The research is carried out from a perspective where personal data protection must be ensured at the highest level accordingly to the GDPR, thus highlighting the challenges therein.

1. Fundamentals of personal data protection

During the past decades, rapid development of modern technology has not only shifted the behavioral patterns of the society, but also given rise to new questions and issues that are in need to be tackled, as it is, for instance, in legal practice, specifically with personal data protection and legislation therein. Currently, across the European Union (hereinafter – EU), personal data protection legal framework is known to be harmonized[1], and as one of the first legal acts known to be developed in 24th of October, 1995, is Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data on the Free Movement of Such Data (hereinafter – Directive 95/46/EC) which pin-pointed the beginning of personal data protection in the EU, as we know it today. [2]

The reasons as of why the need to develop a personal data protection regulation became topical vary. During 1970's an increased use of computers called for personal data protection legislation – certain countries did not hesitate to introduce legislation concerning personal data protection, such as the United Kingdom when it adopted the Data Protection Act in 1984.[3] On contrary, the EU introduced its first legal act only in 1995. During the emergence of the Directive 95/46/EC the Internet was only at its beginning stages of development, however, it was the first legislation to be created regarding data protection and which was binding upon Member States of the EU.[4]

As for the legal basis of personal data protection, after the emergence of the Lisbon Treaty, Article 7 and Article 8 of the Charter of Fundamental Rights of the European Union[5] (EU Charter of Fundamental Rights) recognize the right to privacy and right to protection of personal data, as well as the Treaty of Functioning of the European Union (TFEU) recognizes the right to personal data in Article 16[6]. Prior Lisbon Treaty Directive 95/46/EC was a supplementary means of protecting one's data to personal data legislation in the area of freedom, security and justice (FSAJ), which was exercised through a pillar system - by the first (data protection for private and commercial purposes, with the use of the Community method) and third (data protection for law enforcement purposes, at intergovernmental level) pillar.[7]

While the legal basis for today's personal data protection regulation is considered to be the EU Charter of Fundamental Rights and the TFEU, Directive 95/46/EC has been the

---

[1] European Commission, Protection of personal data, https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/know-your-rights/freedoms/protection-personal-data_en, Accessed on 20th of March, 2020.

[2] European Data Protection Supervisor, The history of the General data protection regulation, https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en, Accessed on 20th of March, 2020.

[3] Peter Carey, Data Protection: Fourth Edition – A Practical Guide to UK and EU Law, Oxford University press,2015, p.1.

[4] EUGDPR, How Did We Get Here?, https://www.eugdpr.org/how-did-we-get-here-.html , Accessed on 6th of April, 2020.

[5] Charter of Fundamental Rights of the European Union, Article 7 and 8, https://www.europarl.europa.eu/charter/pdf/text_en.pdf, Accessed on 20th of March, 2020.

[6] Treaty of Functioning of the European Union, Article 16 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012E/TXT&from=EN, Accessed on 20th of March, 2020.

[7] European Parliament, Personal data protection, https://www.europarl.europa.eu/factsheets/en/sheet/157/personal-data-protection, Accessed on 6th of April, 2020.

"backbone" and the fundamental act in the process of shaping the continuous development of EU regulation in data protection, as it lays down the fundamental principles of data protection that have remained unchanged today - more on the fundamental principles of data protection described in section 1.2. of this paper.

In a contemporary, digitized world, data protection regulation strives towards a world of controlled personal data flow, as data are valuable and can be used for various reasons and protects against much more personal data risks than ever before. The obligation to be compliant with the current regulation has been tailored to be able to be in control of personal data and to protect against modern crimes and modern issues, such as phishing scams, the possibility of being profiled, being subjected to "filter bubbles", online fraud and being a victim of online identity theft, and many more threats that may be possibly faced if personal data become a subject of malicious use.

1.1. The value of personal data

Nowadays, personal data are to be considered the 'gold' of our digital age – claims European Union Agency for Cybersecurity.[8] This fact cannot be denied, as enterprises compete amongst each other on which company will acquire more personal data. The more data an enterprise possesses; the more power it gains. Therefore, more than ever before, online anonymity and ensuring anonymity has gained its importance.

The information or data which are subjected to the struggle of power vary from data on consumer behavior, interests, money spending habits, such as types of products people look at on the Internet, or what they buy and read, what are generally interested in, to even health data and political beliefs about an individual.[9] The information can be used to benefit businesses and to develop more tailored marketing or business development strategies. Information about spending habits or interests may provide businesses with a clearer understanding which people to target with their service or product, as well as other information may become beneficial. Another type of data which can be used for such purposes and is quite popular is contact information data, as the contact details on person, such as e-mail and telephone number, name and surname.

The aforementioned data provide with the opportunity to exercise individually suited targeting, by sending out individual offers and spam emails to sell products and services. "The estimated ARPU (average revenue per user) in digital advertisement, mainly controlled by Google and Facebook, reached $59 per person in 2017"[10], therefore there is no surprise that many businesses exist which solely rely on collecting data and selling them to other businesses who are in need.

The biggest problem which arises in this context is that an individual has no idea where his or her data are, to whom are they given and for what purposes, not being able to be in control of their own personal data. Hence, it is logical to provide an option of browsing the Internet in anonymity in order to be in control of personal data and not be subjected to

[8] European Union Agency for Cybersecurity, the Value of Online Personal Data, https://www.enisa.europa.eu/publications/info-notes/the-value-of-personal-online-data, accessed on 20th of May, 2020.
[9] Ibid.
[10] Ibid.

analysis for commercial purposes on actions carried out on the Internet, especially if one wishes not to be subjected to such analysis. This includes not being "filter bubbled", as individuals have the right to access information they wish to, rather than information they have been presented by artificially. However, while this is the most wide-spread reason, marketing for businesses is only one of the many possibilities on how personal data can be used.

As described, personal data can be acquired legally by providing services and in the process of providing services receiving the information and using the information for marketing or establishing businesses which sell data. However, many illegal businesses and actions also take place with personal data. Which is the reason as of why the fact that one may not know what happens to their personal data is worrisome. Personal data can be used to execute crimes in the name of another individual, or personal data can be acquired illegally, by stealing data from individuals and later on selling the data. One of the biggest threats of such activities known is identity theft, which encompasses many ways in personal data can be subjected to abuse.

1.2.Personal data related crimes: identity theft

Identity theft as a crime, has not been known to emerge recently. Along with the development of technologies, it has been present since 1930's when identities were stolen for voting purposes. Furthermore, the creation of fake identities and identity theft became wide-spread in 1956 when identities were created for illegal immigration. [11] However, due to 21st century technology trends, identity theft has undertaken a new appearance and evolved – identity theft has become more complex in its nature and thus harder to track. Use of the Internet has become a daily habit of the society and most do not become the subject of identity theft, therefore a flawed belief has evolved that one will never be a victim of such crime. But negligence is the main reason as of why it is easy for cybercriminals to carry out the aforementioned crimes.

While stolen data can be used by a thief personally, cybercriminals who steal vast amounts of personal data and further sell the data to other parties are present as well. The majority of transactions occur on the dark web which is a sub-level of "the Internet" and "the Deep web", dark web is not indexed and is limited in access, therefore it can only be accessed by the use of open-source or proxying softwares, such as "Tor".[12] While the dark web may be used for non-malicious purposes, as aforementioned, many illegal transactions, including identity theft and the selling of stolen identities, occur there. As *The Independent* in 2018 had discovered, that "Stolen personal data of UK citizens is selling for as little as £10 on the dark web, offering hackers all the information needed to carry out online fraud and identity

[11] Jake Stroup, A Brief History of Identity Theft, The Balance, Available at: https://www.thebalance.com/a-brief-history-of-identity-theft-1947514, Accessed on 20th of March, 2020.

[12] John Stevenson, All you need to know about Dark web – How to access and what to look out for: How to access and what to look out for, Available at: https://books.google.lv/books?id=OAZuDAAAQBAJ&printsec=frontcover&hl=lv#v=onepage&q&f=false p. 4., Accessed on 20th of March, 2020

theft."[13] But what are the most popular personal data that are being stolen, against which personal data protection is striving to protect against? The answer is as follows: 35% of stolen data are social security numbers, followed by 30% of stolen credit card data,[14] making financial identity theft as one of the most common.

As stated above, identity theft and fraud in the financial industry is a common issue. The most popular types of bank operations that are being targeted are – online payments, card transactions on ATM's or POS devices. But as the banking industry is not still and as any other industry is constantly evolving and moving towards digitization, it poses its own challenges. Identity theft has become more wide spread specifically since the introduction of Internet banking, which consequently provides more opportunities and possible weak points for cybercriminals to tackle. The more complex a service becomes, the higher possibility of a weak-point which can be targeted.

A common practice as a means of acquiring personal data is "phishing". Phishing is stealing one's identity by sending out falsified e-mail addresses which are similar in nature to e-mail addresses of banks or financial institutions, or using false websites which request for an individual to provide with personal information, such as credit card data, PIN codes, social security numbers, etc.[15] Additionally, identity theft can be carried out and information acquired by "pharming" - the use of various illegal softwares, which can be installed on a user's device and which, without the users knowledge, perform different tasks on the device - such softwares are otherwise known as computer viruses. Popularly known computer viruses of such include "Trojan horse", different "keylogger" type of viruses which are installed on the device and store passwords, usernames, banking data that are entered by the keyboard. [16]

> "Some of these virus technologies attack the address bar of the Internet browser and are more advanced than phishing. When customers enter a valid URL address, instead of the valid sites they are re-directed to criminal Web sites. The readdressing to fraudulent sites is realized through infecting the local Domain Name Server (DNS). It includes a change of the specific domain record, which results in directing the customer to a site different from the desired (expected) one."[17]

Overall, identity theft as a crime is to be considered as most wide-spread is in the USA, Australia, South Africa, Canada and the European Union. In 2009, the most critical situation in the European Union could be observed in the United Kingdom, as the commercial banks association (APACS) in the United Kingdom reported losses resulting from fraudulent transactions taking place in online banking had increased by 55% in the first half of year 2006, contributing to 22,5 million pounds in losses by comparing to the previous year.[18] According to the information provided by CIFAS[19], an association in the United Kingdom

---

[13] Anthony Cuthbertson, *Stolen UK identities selling for as little £10 on,* , The Independent, https://www.independent.co.uk/life-style/gadgets-and-tech/news/dark-web-id-value-hackers-cyber-crime-a8683821.html, Accessed on 20th of March, 2020.

[14] Doug Shadel, *Is My Identity on the Dark Web?*, AARP, https://www.aarp.org/money/scams-fraud/info-2018/what-is-the-dark-web.html, Accessed on 20th of March, 2020.

[15] Prof. Silvia Parusheva, Identity Theft and Internet Banking Protection, University of Economics – Varna, Economic Alternatives, Issue 1, 2009, p.44.

[16] Ibid., p. 45.

[17] Ibid.

[18] Ibid.

[19] CIFAS, https://www.cifas.org.uk/, Accessed on 6th of April, 2020.

fighting against fraud and for prevention of fraud, between the period of year 2000 and 2006, online identity theft had grown by 500%.[20]

Although the data presented are from the year 2006 and not the current time at hand, it underlines the importance, rapid growth and topicality of the issue in Internet banking. Identity theft in the online realm is a great threat to financial institutions that constantly must be tackled.

Different solutions to this day have been implemented in order to prevent fraudulent activities, for instance, by introducing more secure authentication ways in online banking, such as by introducing multifactor authentication, with the use of PIN calculators, cards or by supplementing the authentication process with a trust service provider service. Naturally, the identification process must also adapt to changes in the banking industry, and become easier to use, effective and secure as well, however, subjected to digitization, even the authentication process may become a subject of threat.

While ensuring online anonymity is crucial, it must be noted that ensuring online identity for certain actions is equally crucial as well, in order to prevent unauthorized access to data, not be subjected to identity theft and many other reasons as of why. Online anonymity and identity both share a thin line which must be carefully walked on – both crucially necessary, however, clashing in some instances, causing mild confusion.

As online anonymity is crucial, it must be understood that anonymous personal data are not subjected to GDPR. Therefore, the continuing research will put an emphasis on the importance and risks of a user's electronic identity (eID) verification and how online electronic identity and the main idea behind regulation which regulates online electronic identity clashes with GDPR and its aim to give control over personal data for the data subject as well as possible solutions, compliance challenges and personal data protection therein.

1.3. The emergence and role of the GDPR

The initial purpose of Directive 95/46/EC intended for the Directive to tackle personal data protection in physical form – data which is stored physically, such as, health records, employee case files, Curriculum Vitae's, filled out customer forms and other information which can be obtained and stored physically. However, with the rise of technologies and crimes, such as identity theft, that could now be carried out digitally and therefore rising the value of personal data, an organic need has developed for the legislation to evolve and adjust to the current situation, where Directive 95/46/EC did not hold the material scope.

On May 24, 2018, General personal data protection regulation (GDPR) was enforced, which repealed Directive 95/46/EC, and which focuses on personal data protection that are being processed through partially or fully automated means. The GDPR resolved the necessity as it regulates the online realm which could not be reached by the Directive 95/46/EC alone.

One of the first instances where the European Court of Justice (ECJ) came into contact with the challenges that the modern form of digital business brings is the case Google Spain

[20] Prof. Silvia Parusheva, Identity Theft and Internet Banking Protection, University of Economics – Varna, Economic Alternatives, Issue 1, 2009, p.45.

C-131/12[21] (Google Spain case) and Weltimmo C-230/14 (Weltimmo case). [22] Google Spain case is to be considered as one of the landmark cases – it defined what is to be considered as an "establishment."[23] In the light of the Directive 95/46/EC, broadening the scope of the term and giving a rise to other possible gaps that may need to be filled, as new, unprecedented situations were starting to emerge.

In Google Spain case, an individual brought an action against Google Spain, Google Inc. and La Vanguardia newspaper after finding out that typing in his name in the Google search engine showed results of a news article listing a real-estate auction which has been initiated due to personal financial problems and an ongoing process of debt collection.[24] One of the preliminary questions posed to the ECJ was whether the subsidiary company, which is Google Spain, located in Spain and only carries out marketing related actions, is to be considered as an "establishment of the controller". Given the fact that its parent company, Google Inc., is located outside EU - in the US, and which in practice provides with the search results provided by the engine.[25] As well, a question on whether an "equipment is used" in a EU member state under the Directive 95/46/EC and "Whether the rights of erasure, blocking and objection of Directive 95/46 extend to enabling the data subject to address himself to search engines in order to prevent indexing of the data."[26] The Court did rule that Google Spain is to be considered as an "establishment" in the light of the Directive 95/46/EC, Article 4(1)(a), as it engages in activities and is a subsidiary to Google Inc.

> "The processing of personal data by the controller is also "carried out in the context of the activities" of an establishment, even though Google Spain is not involved in the processing at issue […] but rather only in advertising in Spain"[27]

Article 4(1)(a) does not state that the activities should be carried out "by" the establishment, as stated by the Court.

Weltimmo case, on the other hand, was the first case in which a new precedent was created – the application of Hungarian national law for a controller based in another Member State, rising the need for a harmonized regulation in personal data protection. In Weltimmo, a company (Weltimmo) based in Slovakia operated a real-estate website in Hungary, which targeted Hungarian citizens, was comprised in Hungarian, as well as processed and collected Hungarian citizen personal data. The data collected was payment information due to the service which is provided to the citizens – a possibility to advertise real-estate property on the platform in turn for a monthly subscription fee after. However, the first month every new user was given a free trial. Many tried to cancel their subscriptions after the free trial ended, which turned out to be unsuccessful as Weltimmo deliberately ignored the requests and

---

[21] Google Spain SL v. AEPD (The DPA) & Mario Costeja Gonzalez, C-131/12, http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&docid=152065, p.18., Accessed on 6th of April, 2020.
[22] Weltimmo s. r. o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság, Case C230/14, http://curia.europa.eu/juris/document/document.jsf?docid=168944&doclang=EN, p.29. Accessed on 6th of April, 2020
[23] Ibid.
[24] Ibid.
[25] Google Spain SL v. AEPD (The DPA) & Mario Costeja Gonzalez, C-131/12, http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&docid=152065, p.18. Accessed on 6th of April, 2020.
[26] Ibid.
[27] Ibid., p.19.

proceeded with charging the users of the next month's payment.[28] The Court stated that Directive 95/46/EC Article 4 (1) (a) does preclude the use of national data protection laws where it is necessary and a controller is exercising its activity in another Member State. [29] Both of the described landmark cases raised concerns about an individual's ability to control its personal data, as well as exercising its right to privacy in the online realm.

However, the most significant landmark case that highlighted the beginning of the development of the GDPR was case Maximillian Schrems v. Data Protection Commissioner, C-362/14 (Schrems case)[30]. In the Schrems case "adequate level of protection" was defined, as well as the "Safe Harbor" principle was re-evaluated. This particular case showed a very scrupulous approach to "Consent" and the "Right to Access" in personal data protection regulation, as stricter preconditions for personal rights were established. In Schrems case, Maximillian Schrems, an Australian student, sued Facebook Inc. in the High Court of Ireland, due to the fact that Facebook Inc. allegedly transmitted data from Ireland to the USA which consequently permitted access to the data for the National Security Agency (NSA) of the United States of America.[31] The Court found that Article 25 (6) of the Directive 95/46/EC does not explicitly require for non-EU countries to provide with the level of protection as the wording in Directive 95/46/EC provides that a third country should provide with an "adequate level of protection" in the light of Article 2 of the Directive 95/46/EC and for the purpose of protecting an individual's basic right of privacy and freedom.[32] The Court found the Safe Harbor principle as not viable, as the NSA had access to personal data that were transmitted to the USA:

> "Decision 2000/520 does not contain sufficient findings regarding US measures which ensure adequacy by reason of domestic law or international commitments. Rather, it enables interference with fundamental right to respect for private life of persons whose personal data is or could be transferred from the EU to the US."[33]

And thus, the EU Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation or the GDPR) was developed.[34] The GDPR was

---

[28] Weltimmo s. r. o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság, Case C230/14, http://curia.europa.eu/juris/document/document.jsf?docid=168944&doclang=EN, p.29. Accessed on 6th of April, 2020

[29] DPO, Summaries of EU Court Decisions Relating to Data Protection 2000-2015, Data Protection Officer, 2000-2015, p. 51., https://ec.europa.eu/anti-fraud/sites/antifraud/files/caselaw_2001_2015_en.pdf, Accessed on 6th of April, 2020

[30] Maximillian Schrems v. Data Protection Commissioner, Digital Rights Ireland, C-362/14, http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=23555, Accessed on 6th of April, 2020.

[31] Ibid.

[32] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995, Article 25 (6), http://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN, Accessed on 6th of April, 2020

[33] DPO, Summaries of EU Court Decisions Relating to Data Protection 2000-2015, Data Protection Officer,2000-2015, p. 48., https://ec.europa.eu/anti-fraud/sites/antifraud/files/caselaw_2001_2015_en.pdf, Accessed on 6th of April, 2020.

[34]Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

developed in order to enhance individuals rights and the possibility to exercise individual's rights in regards to personal data protection when in potential presence of data abuse. GDPR is the first harmonized, directly applicable Regulation regarding personal data protection in the European data protection law's history. As the European Commission had found out, nearly 90% of EU citizens expressed a wish for their rights to be harmonized across the Europe in this matter - the European Commission comments on the development of GDPR:

> "The regulation (GDPR) is an essential step to strengthen individuals' fundamental rights in the digital age and facilitate business by clarifying rules for companies and public bodies in the digital single market. A single law will also do away with the current fragmentation in different national systems and unnecessary administrative burdens."[35]

1.3.1. General concepts of data protection

Before diving into the world of personal data protection and to understand how the legislation must be interpreted, it is crucial to understand the fundamentals and the basic concepts of data protection. The first and the most important term to understand is the term itself - "personal data" - what constitutes as personal data and what is the topic of subject that is regulated under data protection laws?

Article 4 (1) of the GDPR defines "personal data" as follows:

> "'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person"[36]

the definition of "personal data" encompasses 4 basic and crucial elements which are to be distinguished and understood - "any information"; "relating to"; "identified or identifiable"; "natural person". In order to determine if the information is considered personal data, it must be weighted whether, by using all reasonable means, a person can be identified - in order to determine if the chosen means are reasonable, the economic costs, time and technology available to identify a person must be taken into account. [37]Furthermore, it must be noted that the data of legal persons is not covered by the GDPR, however, in certain instances, personal data of persons associated with a legal entity can be subjected to GDPR. For instance, personal data of employees who represent a legal entity are to be protected, as well as personal

---

https://eurlex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN, Accessed on 6th of April, 2020.

[35] European Commission, Data protection in the EU, https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en, Accessed on 6th of April, 2020.

[36] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) , https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN, Article 4(1), Accessed on 7th of April, 2020.

[37] General data protection regulation, Intersoft consulting, consolidated version, Recital 26, https://gdpr-info.eu/recitals/no-26/, Accessed on 7th of April, 2020.

data of board members of a legal entity in some instances where their personal data is disclosed to other entities or natural persons.

The terms "Data controller", "data processor" and "data subject" are crucial to be distinguished and understood when in discussion on personal data protection as well. Data controller is to be considered any natural or legal person, organisation or public authority which processes personal data and determines the reason of processing, means by which data are processed. "Data processor" processes personal data on behalf of the data controller, meaning that data controller determines how much data and how the data will the processor process. Lastly, "data subject" is a natural person whose personal data are subjected to processing.[38]

Many have developed the misconception that personal data processing constitutes active engagement with personal data that are in controller's possession, as, for instance, by carrying out analysis from the data collected or disclosing personal data to unauthorised third parties, etc., however, processing is not limited to activities as such. Storing, collecting, organising, structuring, erasing and any other operation that can be carried out with personal data by partial or fully automated means, as well as non-automated means, constitutes as data processing.[39] Meaning that a simple employment contract which encompasses names of the signing parties might also constitute as personal data, especially if social security numbers are disclosed.

In other words – while the GDPR does not protect legal entities and therefore it might be tempting to believe that the GDPR does not apply to enterprises, in reality, almost every legal entity processes personal data. If a company's clients are only legal entities, the company would be tempted to think so, however, it may have employees whose personal data must be protected, as they are natural persons, too.

Personal data protection is not only limited to clients and their data processing – data protection covers every single individual's data protection without exemptions. Above all, the fundamental message of the GDPR is to prohibit any personal data processing without a legal ground and to strengthen the protection of individual's rights. As this work puts an emphasis on the financial sector and personal data protection therein, the following work will put an emphasis of legal entity compliance with GDPR.

1.3.2. Legal grounds for processing data

When thinking about a company's compliance to GDPR, principles of personal data protection laid down in Article 5 of GDPR must be respected, as for instance, one of the first factors to consider is whether all of the obtained data are necessary, or in other words – has the "minimization principle"[40] been taken into account, followed by weighing out whether all the necessary personal data being processed hold legal ground of processing. Legal grounds for data processing are to be found in Article 6 of GDPR:

---

[38] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) , https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN, Article 4, Accessed on 7th of April, 2020.

[39] ibid., Article 4 (2)

[40] Ibid., Article 5 (c)

" [..] (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes; (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; (c) processing is necessary for compliance with a legal obligation to which the controller is subject; (d) processing is necessary in order to protect the vital interests of the data subject; (e) processing is necessary for the performance of a task carried out in the public interest [..]; (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject [..]"[41]

As it can be seen, various legal grounds for data processing exist, subsequently, each of the grounds have their own criteria in order to fulfill them. For instance, a legitimate interest as a legal ground has been introduced due to the fact that legal entities may need to process personal data directly related to carrying out business activities. Whether it is direct marketing exercised on an existing client, to prevent crime – fraud, cyberattacks to IT systems, or to carry out internal analytics for business development and service improvement purposes, [42] or, in order to fulfill an obligation of a contract. It is logical, however, the problem arises when the personal data is used for other purposes than the one alone.

Each personal data that is in the possession of a company is to be supported by a separate legal basis for each data processing activity. After the GDPR was enforced in May of 2018, a general trend of various companies all over the world to start using consent as the legal basis for personal data processing by asking permission to most of the data processing activities carried out in the company was observed, however, it is important to note that consent is one of the weakest legal basis on which to process personal data. The reason for this is that personal data which is based on the legal grounds of consent can be easily revoked according to Article 7 of GDPR "Conditions for consent"[43] and such an option is to be ensured by a company, as this is one of the data subjects rights provided in the Regulation.

1.3.3. Data subject rights

Data subject rights that are described in Articles 12-22 of the GDPR[44], have derived from Article 16 of TFEU[45] and Articles 7 and 8 of the Charter of Fundamental Rights of the EU "respect for private and family life" and "protection of personal data"[46]. Each controller must ensure that an individual, data subject is provided with the opportunity to exercise rights

[41] Ibid., Article 6 (1)
[42] European Commission, What does "grounds of legitimate interest" mean?, https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/what-does-grounds-legitimate-interest-mean_en, Accessed on7th of April, 2020.
[43] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) , https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN, Article 7, Accessed on 7th of April, 2020.
[44] Ibid., Articles 12-22, Accessed on 7th of April, 2020.
[45] Treaty of Functioning of the European Union, Article 16 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012E/TXT&from=EN, Accessed on 7th of April, 2020.
[46] Charter of Fundamental Rights of the European Union, Article 7 and 8, https://www.europarl.europa.eu/charter/pdf/text_en.pdf, Accessed on 7th of April, 2020.

mentioned in the Regulation, to ensure control over personal data, as well as to ensure control over personal data where it is necessary – for instance by not allowing to deploy cookies on the user's device which collects data on the behavior of the data subject. The balance between data subject's rights, data minimization principle, providing services and ensuring adequate safety measures to protect data subject personal data and, at the same time, to adequately identify an individual are a never-ending constraint, as some may come in conflict with other. This particular issue is to be looked at further in the work, moreover – what are the rights that data subjects can exercise?

Firstly, data processing that is carried out must be done in a transparent matter, meaning that the data subject holds the right to be informed about any data processing activities that are ongoing in a company. Therefore, privacy policies and notices are prepared by institutions in order to be transparent and inform individuals of their data processing activities. Not all information is publicized, as, for instance, the notices do not list particular individual names and data that is in the hands of an entity, therefore an opportunity for the data subject to request for access to information has to be ensured. When the data subject submits a notice (request for access to personal data), the company must, usually within 30 days of time, provide with the requested information or reply by solid arguments on why the information cannot be provided.

Moreover, the data subject holds the right to request for rectification, data erasure, restrict or object to data processing which are different in their own nature while may sound similar. The right to rectification ensures an up to date and accurate personal data to be in hand of the controller, while erasure is for the data subject to request the deletion of personal data in the possession of an entity, however, the right to object and right to restrict processing are rather similar, as both challenge the data processing activities of the controller.

Finally, the right to data portability ensures the opportunity for personal data to be safely transferred to another service provider, for instance, if a person decides to change the bank, the data subject may request for safe data transfer to the new bank of which the data subject has become a client of. [47]

Whereas data portability is a right that can be exercised, it raises other issues, as for instance, banks must ensure an appropriate level of security for data transfers, which may bring up many other unprecedented security threats. Any fulfillment of data subject rights can give rise to new security threats, for that matter, however, one example in which new security threats have emerged is by exercising the right to access in Article 15 will be specifically looked at in the next sub-chapter.

1.3.4. Art. 15 Right of access by the data subject

Article 15 of the GDPR states as follows:

> 1. "data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information: […] 3. The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a

[47] Ibid.

> reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form. […]"[48]

therefore, in accordance with the Articles provisions, the controller must ensure the opportunity to exercise such a right and to respond accordingly. However, while it may seem as simple as a request for information and providing of such information, it is the controller's responsibility to transfer the personal data to the right person. Recital 64 of the GDPR affirms:

> "The controller should use all reasonable measures to verify the identity of a data subject who requests access, in particular in the context of online services and online identifiers. A controller should not retain personal data for the sole purpose of being able to react to potential requests."[49]

As it can be seen, the controller is responsible for the identification of the person submitting a request for information, taking into account that the controller cannot retain personal data for the purpose of responding to the requests. What does that mean? This raises new issues and loopholes in this matter.

A research on "Personal Information Leakage by Abusing the GDPR "Right of Access"[50] has been carried out in May 2019, by students of Hasselt University, Expertise Centre for Digital Media, Law Faculty, where this issue was tackled more in detail. An experiment was carried out by sending out data request emails with fake identities to 55 organizations from the financial, entertainment and retail industry. Unfortunately, 15 out of 55 organizations disclosed sensitive and personal data "including but not limited to financial transactions, website visit histories and timestamped locations. Exercising the "Right of Access" while impersonating a data subject is therefore an appealing attack for criminal adversaries."[51]

The reasons as of why the aforementioned 15 organizations disclosed personal data without an individual's identification vary, for smaller and medium sized businesses it is the cost of implementing advanced approaches. It was concluded that 41 out of 55 organizations allow to submit a data request through an email and only 5 require to show an ID, while only 2 call the data subject to reassure whether a data request has been submitted, and it is a rather unpleasant statistic.[52]

From the financial institutions alone, the following data was disclosed without identification: "ID card number, list of timestamped financial transactions, customer ID, telephone numbers, place of birth, partial debit and credit card numbers, list of products purchased from the financial institution, and account numbers."[53] The research was carried out

---

[48] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) , https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN, Article 15, Accessed on 15th of April, 2020.
[49] General data protection regulation, Intersoft consulting, consolidated version, Recital 64, https://gdpr-info.eu/recitals/no-64/, Accessed on 15th of April, 2020.
[50] Mariano Di Martino, Pieter Robyns, Winnie Weyts, Peter Quax,
Wim Lamott1, and Ken Andries, *Personal Information Leakage by Abusing the GDPR "Right of Access,* Hasselt University, Expertise Centre for Digital Media, Law Faculty, May, 2019.
[51] Ibid., p.12.
[52] Ibid., p.5.
[53] Ibid., p.9.

in the first quarter of 2019, meaning that not long ago, financial institutions were vulnerable enough to disclose information to unauthorized persons with faked emails and ID cards, emphasizing the need for secure identity verification tools in order to avoid such instances., owever, providing with the opportunity for individuals to control their personal data. Recital 64 of the GDPR and the importance of identifying the data subject properly create a quite narrow field in which to operate, as they might overlap in some instances.

2. Online Identity and eID verification

The first part of this work provided an insight in EU data protection regulation and presented the fundamental reasons as of why ensuring control over personal data and to protect personal data is crucial in the digital era. It also introduced the topicality of electronic identity verification as a tool, mostly to newly emerging digital trends - providing certain services remotely requires to identify the end user in order to avoid disclosing information to an unauthorised person or in order to avoid the occurrence of a cybercrime such as identity theft. On contrary, ensuring the opportunity of an individual to be in control of personal data provides with the opportunity to not be subjected to analysis of personal data and the acquisition of data without permission. Furthermore, even if personal data protection measures have been implemented, the compliance, as for instance, executing the obligation to respond to personal data requests, has given rise for a need to correctly and safely identify individuals placing such requests by not breaching one's right to exercise the rights laid down in GDPR.

However, online identity and the importance to identify an individual remain in cases such as with Article 15, but not limited to. Simply put, "eIDV (Electronic Identity Verification) makes use of publicly available data as well as private databases to quickly verify the identity of an individual."[54] And the means as to verify ones identity and levels of identity verification vary, as identity verification can be carried out by receiving various types of data. For instance, as simple as by providing data of birth and social security number and as far as by asking to provide specific information which is compared to information available in databases of state authorities.

As it had been concluded, one must be careful to identify an individual in terms of data requests as the data controller is prohibited to retain more data than necessary for such purposes, therefore the right method of identity verification must be chosen carefully and wisely. Some opt for sending a specifically generated serial number or code to an individual's mobile device and therefore only providing two-factor authentication as the only means of making sure the same person carrying out an action is indeed the one who is receiving the SMS. Others, before providing services, may ask for a secret password, or if it is a platform, such as an internet platform for banking services, in order to log in, a bank might use a trust service provider service which ensures qualified website authentication. A certificate for website authentication is "an attestation that makes it possible to authenticate a website and links the website to the natural or legal person to whom the certificate is issued"[55]. Using a certificate for website authentication is a type of a secure authentication, moreover, the levels of authentication must be distinguished in their nature and levels of assurance.

As for the legal framework of electronic identities and communication, five main regulatory acts must be taken into account: Regulation (EU) No 910/2014 or the eIDAS Regulation, Directive (EU) 2015/2366 or the PSD2, Regulation (EU) 2016/679 otherwise known as the GDPR, the 4th amendment of the Anti-Money Laundering Directive (EU) 2015/849 and the ePrivacy Directive 2017/03 (COD). A balance between all five regulations

[54] Jake Frankenfield, eIDV (Electronic Identity Verification), Investopedia, https://www.investopedia.com/terms/e/eidv-electronic-identity-verification.asp, Accessed on 1st of May, 2020.
[55] European Union Agency for Network and Information Security, Qualified Website Authentication Certificates Promoting consumer trust in the website authentication market, 2015., p.22.

must be found, as well as compliance must be ensured in order to safely provide services remotely, while accordingly identifying the end-customer.

2.1. eIDAS, PSD2 and 4th Amendment of the AMLD

To get an overall understanding of the legal framework of electronic identities and communications, see *Annex 1. "Timeline of the European legal framework for digital identities and communication"* attached to this paper which provides with an overview of the relevant regulatory acts and the timeline of regulation's entry into force.

Electronic identification (eID), authentication and certificates in the EU are regulated by Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (hereinafter - eIDAS Regulation). eIDAS is the fundamental of eID and as a Regulation, it is directly applicable to all Member States, and

> "In support of the European Commission's Digital Single Market (DSM) initiative, eIDAS aims to facilitate the smooth flow of commerce in the EU through harmonization of law, transparency, security, technical neutrality, cooperation and interoperability."[56]

In ensuring the fulfillment of the fundamental aim of the Regulation, the Regulation not only standardizes the use of eID, but also defines what are electronic Trust Services (TS) and describes the validity and levels of electronic signatures.[57] The previous Electronic Signatures Directive 1999/93/EC did not clearly define the use of eID, therefore eIDAS elaborates, apart from putting emphasis on electronic signatures alone. In short, eIDAS can be divided in two areas of electronic identification and trust services, by both holding separate complementary regulatory acts that have been adopted.

Interestingly, eIDAS was developed before the emergence of GDPR, therefore when eIDAS references to personal data protection laws, it references to Directive 95/46/EC not the GDPR as we know it today and thus accordingly impacting eIDAS. However, The 4th Amendment to the anti-money laundering Directive (AMLD) especially is applicable for financial institutions of banking service providers, as it provides that the parties of a transaction carried out must be properly identified.[58] The 4th Amendment of AMLD lays down guidelines and stricter provisions for digitized Know-Your-Customer (KYC) processes, including dealing with cross-border third party electronic identity verification services for KYC processes, such as the Estonian web and mobile identity verification service Veriff OU, which helps to meet the KYC requirements.[59]

Moreover, PSD2 Directive or Directive (EU) 2015/2366[60] is the second Payment Services Directive, a revised version of the Payment Services Directive which came into force for more

---

[56] Scrive, eIDAS: Standardising Digital Identity in the EU, https://www.scrive.com/eidas-electronic-identity-in-the-eu/, Accessed on 10th of May, 2020.
[57] Ibid.
[58] European Commission, eIDAS & 4th Anti-Money Laundering Directive - a short update, https://ec.europa.eu/futurium/en/content/eidas-and-proposal-amendment-4th-anti-money-laundering-directive, Accessed on 15th of May, 2020.
[59] Ibid.
[60] Directive (EU) 2015/2366 of the European Parliament and of the Council

than ten years ago – on 25th of December, 2017.[61] PSD2 impacts and transforms the European financial eco-system vastly, as it aims to regulate third-party service provider access to payment accounts which are managed in online banking by banks.[62] Ultimately, PSD2 is tailored towards the developing financial industry, specifically towards API banking and it's posing challenges in payment traffic.[63] In short, banks are encouraged to securely transfer data to third party services, such as, e-Commerce stores and platforms, allowing them to make payments for individuals rather than redirecting to another service, such as PayPal or Visa.[64] Furthermore, this could possibly mean that individuals or businesses who own several bank accounts could access all the account information in one place, however, all of this comes with a notion of a secure user authentication and identity verification, as it strengthens the importance of it.[65]

On August 2016, Regulatory technical standards (RTS) for strong customer authentication (SCA) and secure communication (CSC) otherwise known as Commission Delegated Regulation (EU) 218/389[66] was published, which is a supplementary act to the PSD2 Directive. The Consultation Paper for RTS on SCA and CSC lays down specific requirements which must be fulfilled in regards to secure authentication, as for instance, is done by Article 2 of the Consultation Paper "General authentication requirements"[67] which requires payment service providers to ensure transaction monitoring mechanisms to detect unauthorized transactions. However, Chapter III "Security measures for the application of strong customer authentication"[68] elaborates in detail on the meaning of SCA referred to in PSD2 Directive, Article 97(1).[69] SCA according to PSD2 means ensuring authentication with more than two of the following elements: 1) knowledge – information that is known only by the user, e.g.,

---

of 25 November 201 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366&from=EN, Accessed on 17th of May, 2020.

[61] European Commission, Payment Services Directive 1 – Directive 2007/64/EC, https://ec.europa.eu/info/law/payment-services-psd-1-directive-2007-64-ec/law-details_en, Accessed on 17th of May, 2020.

[62] Andrea Müller, eIDAS, PSD2, GDPR & Co The European legal framework for digital identities and communication, 2018, https://asquared.company/public/asquared-blog_post_en_2018-02-01_eidas-psd2-gdpr-u-co_v1.pdf, p. 5., Accessed on 17th of May, 2020.

[63] Ibid.

[64] Transferwise, PSD2 Explained: What is it and why does it matter?, https://transferwise.com/gb/blog/what-is-psd2, Accessed on 17th of May, 2020.

[65] Ibid.

[66] Commissioni delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R0389&from=EN, Accessed on 17th of May, 2020.

[67] Ibid., Article 2.

[68] Ibid., Ch. III.

[69] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 201 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366&from=EN, Article 97(1), Accessed on 17th of May, 2020.

password; 2) Ownership – something in the users possession, e.g., token, mobile device; 3) Inherence – data about the user's identity, e.g. voice recognition, fingerprint. [70]

Together and individually, authentication elements which form authentication methods can be categorized in levels of assurance, which signify the trustworthiness of the person identified.

2.2.Authentication levels of assurance

Authentication is considered as an electronic identity verification mean, however, the different levels of authentication are widely different in terms of the level of security and assurance, meaning that all give a different degree of assurance and confidence in the identity of the presented person. The more a website or a platform stores sensitive information, the stronger and more reliable electronic identity verification means must be applied. eIDAS Regulation defines authentication as "'an electronic process that enables the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form to be confirmed"[71].

Authentication assurance levels most commonly are divided in 4 levels: level 1 - low level authentication, two-factor authentication, multi-factor authentication and the 4th being the highest level of assurance. Level 1 authentication mainly requires for a password and a username, and does not identify a person accessing the website or platform, which is the least secure way to protect a user account against a cyberattack and data theft. Whereas two-factor authentication requires a second level of confirmation apart from the standard password and username, for instance, by sending out an automatically generated PIN or code to the person's e-mail or mobile device. Multi-level authentication usually includes Biometric data, such as a fingerprint scan on a mobile device combined with a PIN code. And lastly, the highest level of assurance is the level in which qualified certificates are to be used in order to identify an individual by using Qualified Trust Service Provider (QTSP) services. [72] However, eIDAS has defined eID levels of assurance, which differentiate the level of trust in identity verification in 3 three levels of "Low", "substantial" and "high", and the requirements and definitions have been defined through Commission Implementing Regulation (EU) 2015/1502 Annex 2 .[73] The Regulation defines the degree of confidence in the claimed identity of a person.[74]

---

[70] Thales, PSD2 - Double down on security with 2‑factor authentication, https://www.thalesgroup.com/en/markets/digital-identity-and-security/banking-payment/digital-banking/psd2/strong-customer-authentication, Accessed on 20th of May, 2020.

[71] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN, Article 3 (5), Accessed on 15th of May, 2020.

[72] GCN, The 4 levels of Authentication in a Mobile World, https://gcn.com/Articles/2013/02/12/4-levels-mobile-authentication.aspx, Accessed on 15th of May, 2020.

[73] Niko Tsakalakis, Sophie Stalla-Bourdillon and Kieron O'Hara, What's in a name: the conflicting views of pseudonymisation under eIDAS and the General Data Protection Regulation, Open Identity Summit 2016, Available at: https://subs.emis.de/LNI/Proceedings/Proceedings264/167.pdf, p.168, Accessed on 1st of June, 2020.

[74] Marijke De Soete, eIDAS Regulation – eID and assurance levels – Outcome of eIDAS study, Security4Biz (Belgium), 24 June 2015, https://docbox.etsi.org/workshop/2015/201506_securityweek/eidas_thread/s03_eid/security4biz_de_soete.pdf, Accessed on 1st of June, 2020.

As mentioned beforehand, using certificates for website authorization is the highest level of authentication and identity assurance, due to the fact that it uses certificates in the process of electronic identity verification. However, one must understand the technical functionality of certificates in order to understand why it is considered the highest level of assurance.

eIDAS defines certificates for website authentication as "an attestation that makes it possible to authenticate a website and links the website to the natural or legal person to whom the certificate is issued"[75]. Issuing certificates provides an equal effect as of a person showing an ID in order to provide a link between the person standing in front and the ID for the purposes of gaining access to certain information or to be eligible to provide a handwritten signature on a document.

The foundation of an electronic identity and therefore also an electronic signature is public key cryptography technology where each individual is issued a key pair with a public and a private key, therefore an individual who owns a matching private key to a public key may sign a document, as the person is considered to be linked to the specific identity. [76]A real life analogy would be the confirmation procedure of an ID card's information presented by a person and its similarity to the information in registers. However, since the identification process occurs remotely, in order to guarantee the highest assurance of the person's identity, or the "ID card's holder", using the analogy of the real life example given, a trusted certification authority or Certification Service Provider (CSP) certifies the link in a public key certificate. [77] A CSP is a type of a Trust Service Provider (TSP) which is eligible to bear and issue certificates, furthermore, TSP's are listed and categorized by Member States and in order to be presented with such a title

> "Providers of eIDAS-compliant services must undergo testing by dedicated conformity assessment bodies to be permitted to provide trust services and to be included in the list of national trust service providers. The list is kept by a national authority; in Germany the Federal Network Agency is responsible for this task. The Trusted List of Trusted Lists (LOTL) provides a Europe-wide overview of all audited and approved national providers."[78]

Most of the EU Member States already have incorporated electronic identity cards which bear digital certificates, more often than not also qualified certificates, and therefore one may not need to additionally seek for a CSP in order to create a qualified certificate. [79]

Furthermore, Article 25 of the eIDAS draws parallels between a qualified electronic signature (QES) and a handwritten signature by equating both in terms of their legal effect, therefore, providing that certificates created in Member States (MS) are to be recognized

---

[75] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN, Article 3 (38)., Accessed on 15th of May, 2020.
[76] European Union Agency For Network And Information Security, Security guidelines on the appropriate use of qualified electronic signatures Guidance for users, December 2016, p.15.
[77] Ibid., p.16.
[78] Andrea Müller, eIDAS, PSD2, GDPR & Co The European legal framework for digital identities and communication, 2018, https://asquared.company/public/asquared-blog_post_en_2018-02-01_eidas-psd2-gdpr-u-co_v1.pdf, p. 3., Accessed on 15th of May, 2020.
[79] Ibid., p. 32.

across all MS's in the European Union. [80] This particular Article is significant in terms of the fact that it means a signature can be created without the presence of a signature card held by the user but rather the signature file can reside on secure servers of a QTSP/TSP, which in turn greatly lessens the regulatory and technical barriers in the use of QES.[81] "However, this does not mean that all hurdles have been overcome; issuing the certificate for a QES still requires the user's identity check in presence or an electronic identification device at security level "substantial" or "high"'"[82].

And this is where GDPR poses its challenges, as it can only be stipulated whether the technology on which electronic identification is to be carried out is reliable from the perspective of data protection. The challenges of identity verification in the process of issuing certificates as well as in the process of using such e-services that provide are to be described further in the work by carrying out a case study on two e-service providers and a QTSP.

2.3.Trust Services, E-services and GDPR

Prior eIDAS Regulation, eSignature Directive 1999/93/EC was in place, which established the legal framework of electronic signatures in the European Union. [83] Prior the eSignature Directive, e-signatures were not recognized, as only handwritten signatures were considered valid. The recognition of e-signatures was crucial for the purposes of a EU internal market and the free movement of goods, and thus the conclusion of trans border agreements. While a document can be signed by hand, the opportunity to use e-signatures in order to sign documents opens possibilities to carry out such actions remotely in a fast and efficient manner. However, the introduction of e-signatures meant also other concerns which arose, such as, the uncertainty of security and the validity of the signee. [84] Therefore, for an e-signature not being sufficient enough, other trust services, such as a time-stamp, electronic seal, electronic delivery, legal admissibility and website authentication was needed. If such elements were not ensured, individuals otherwise would be reluctant to use such services, which is one of the reasons as of why eIDAS was developed, as described beforehand.

While certified website authorization is considered the safest means and as the highest assurance of identity verification, a QTSP/TSP must ensure that the provided Trust Service (TS), as well as any other electronic identification schemes must be GDPR compliant. Electronic identification schemes can be executed by a government institution, third party or a QTSP/TSP - a full list of Trust Services can be found on the European Commission's website, named as the "EU Trusted list"[85]. Most Member States have a listed Trust Service, as for instance, in Baltics, a wide-known QTSP is SK ID Solutions AS which has developed SmartID –allowing individuals to sign documents with a qualified electronic signature which also possesses a qualified time stamp. And as the QTSP possesses the certificate for a

[80] Andrea Müller, eIDAS, PSD2, GDPR & Co The European legal framework for digital identities and communication, 2018, https://asquared.company/public/asquared-blog_post_en_2018-02-01_eidas-psd2-gdpr-u-co_v1.pdf, p. 3., Accessed on 15th of May, 2020.
[81] Ibid.
[82] Ibid.
[83] European Commission, Trust Services, https://ec.europa.eu/digital-single-market/en/trust-services, Accessed on 18th of May, 2020.
[84] Ibid.
[85] European Commission, Trusted list browser, https://webgate.ec.europa.eu/tl-browser/#/, Accessed on 15th of May, 2020.

qualified time seal – the SmartID is considered to be viable in terms of using it as the highest level of authorization, because it uses qualified certificates in the process of identity verification. [86] Additionally, it is the only QTSP in EU which operates and issues certificates in more than one Member State. In order to become a QTSP/TSP, the service provider is subjected to strict regulatory means, including various cybersecurity standards that must be fulfilled, however, taking into account that eIDAS and PSD2 have been developed prior GDPR, there are challenges that electronic identification schemes are facing in regards to GDPR.

Apart from Trust Services, on the surface it may seem that many e-service providers offer the exact services that many QTSP provide, as it is with the case of ensuring a platform for signing documents electronically, as for instance, Dokobit, DocuSign, Adobe Sign, Penneo, Lahdes, and other e-signing platforms do. QTSP issue certificates, ensure the possibility to create an electronic signature while the aforementioned e-services as such provide the opportunity to actually sign a document. The platforms are not considered TS as they have not been granted the status of a QTSP. Such e-signing platforms are able to provide with an opportunity to sign a document in a legally binding way despite not being a QTSP. This is possible due to the fact that these services use certificates from QTSP in their region in order to verify one's identity.

The e-service providers, nevertheless, do have to comply with GDPR in order to provide such services. An e-service provider as such is very unlikely to be a QTSP, on contrary, a QTSP can provide e-services in addition to issuing certificates. A great example is a QTSP in Romania called DigiSign Certification Authority which also provides an option to install a software DigiSigner that allows to sign documents with electronic signature. From the perspective of personal data protection, a QTSP which offers e-services in addition is more secure, as it eliminates any risk of a third party e-signer provider not being GDPR compliant.

Since PSD2 and eIDAS require for third party service providers and QTS/QTSP to implement the highest security and monitoring measures, as well as to be GDPR compliant, in practice, it might appear as a challenge for businesses. In order to understand how particular QTSP and electronic identity verification third party services tackle these challenges, further sub-paragraphs will carry out a case study on the following services: SmartID which is the largest QTSP in the Baltics, Dokobit – an e-signing platform, Gov.UK Verify – a government owned eID scheme and Verify – a private, third party electronic identity verification provider.

2.3.1. Case Study: SmartID in the Baltics

SmartID is an electronic identity service which is provided by SK ID Solutions AS which is a QTSP established in Estonia. SmartID is the only Certification Authority which can issue certificates in three member states at once, namely, Estonia, Latvia and Lithuania. Consequently, SmartID as an integration can be used by all entities which operate in the aforementioned countries.

As SK ID Solutions explain, Smart-ID is based on principles of public key cryptography, which was described beforehand in the work. "Compared to other possible user authentication technologies, such as PIN calculators or one-time-use PIN codes sent over the SMS channel,

[86] European Commission, Trusted list in Estonia, https://webgate.ec.europa.eu/tl-browser/#/tl/EE, Accessed on 15th of May, 2020.

the PKI and digital signature approach gives the following benefits: high level of security, non-repudiation of operations, strong authentication and signatures recognized all over the EU."[87] Moreover, SmartID uses two factor authentication by authenticating the device (inherence) and something that is known only to the user, which is a PIN (knowledge).

SmartID recently provided with the opportunity to create a SmartID account remotely, which is a great advancement, as up until the year 2019, registration could only be carried out in person and physical identification. The registration process is carried out as follows: user installs SmartID, using NFC technology scans the ID card and registers the biometric information it holds on the user, takes a self-portrait in order to identify the user standing in front of the device, creates 2 PIN codes and completes the registration. SK ID solution to provide the opportunity to register the qualified account remotely as it uses biometric data which is encrypted in an ID document that has been issued in the European Union. [88]

E-Passports which contain biometric data in the European Union were first introduced in Sweden, in 2005, furthermore, the European Council issued a decision which stated that until 28th of June, 2009, all Member States must introduce the use of E-Passports, which included biometric data, containing fingerprints. This particular decision was challenged by data protection specialists in the EU, giving more reasons for a need to develop a new regulation, thus GDPR. [89] The measures implemented regarding security and protecting the biometric data solely rely on each country individually.

Both – state issued ID documents and certificates issued by a QTSP which is a Certification Authority are trustworthy. All of the necessary steps to comply with GDPR and eIDAS have been taken and overall, SK ID Solutions is a great example on how to comply to regulations that have been imposed by the European Union, while continuing to rapidly expand. However, it raises a discussion of a philosophical nature on whether technology which replaces the individual identifying a person physically can be replaced. Many possibilities exist as to how an identity can be faked by scanning stolen ID cards or in the self-portrait step by photographing a photo rather than the face of the person creating the profile. More on this topic later in the work.

2.3.2. Case Study: Dokobit

Dokobit is an e-service which provides with the opportunity to sign documents electronically. Dokobit currently fully operates in 9 member states of the EU – Latvia, Lithuania, Estonia, Finland, Germany, Poland, Spain, Portugal and Iceland.[90] Dokobit is not a QTSP, however it uses QTSP issued certificates for electronic signatures and identity verification. As mentioned before, e-services must be GDPR compliant, as they have a high risk of data breach – many platforms store signed documents in a cloud or on servers, which must be secured properly, as well as the signing procedure must be ensured accordingly so that an unauthorized party could not access the documents that have been signed or sent. This case study will look at the measures that Dokobit has taken in order to be GDPR compliant.

---

[87] SK ID, SmartID, https://www.skidsolutions.eu/en/services/smart-id/, Accessed on 20th of May, 2020.
[88] SmartID, https://www.smart-id.com/lv/, Accessed on 20th of May, 2020.
[89] Tamas Szadeczky, Enhanced functionality brings new privacy and security issues – an analysis of eID, Masaryk University Journal of Law and Technology, p.10.
[90] Dokobit, https://www.dokobit.com/lv/, Accessed on 20th of May, 2020.

During the registration phase of Dokobit, it has ensured the highest level of used identification and authentication – the possibility to only register with a SmartID or a nationally issued electronic signature or an eID card. This particular method ensures the validity of the individual which is creating the profile, and thus linking the profile to an identified person, meaning that no other person can access the profile without holding the eID or SmartID, as it is in the case with Baltic States.

Dokobit ensures two elements which are described in the SCA: 1) Knowledge, which is a personal ID number to activate SmartID, for instance, and; 2) Ownership, which is the device on which has the SmartID or eID been established. However, Dokobit fails to eliminate all possible risks in verifying the receiving end of the document. When the registered and identified individual signs a document, the person is able to add other signatory parties to the document and send out an invitation to sign the document via three methods: either using a person's email, or a personal ID number. There seems to be no problem when a personal ID number is entered to send the document, as it can be sure that the document will be sent to the respective account owner which has been registered with the particular ID number. In contrast, if the document is to be sent by only providing the email address of the receiving end, the document might end up disclosed to the wrong party, due to human error, signifying a data breach. For instance, if one party signs the document and sends it to the wrong e-mail address, the receiving party can automatically access the document through the platform, without any other layer of assurance that the document indeed has been delivered to the right party.

This particular flaw could be eliminated by ensuring a two or more factor identification method. Meaning that in order to send a digitally signed document to other parties, one must provide at least two elements, for instance, two of the following: personal ID number, e-mail or telephone number. After the document has been signed, the receiving end only is able to access the document if both elements match and belong to the receiver. The connection between both can be ensured in various ways – one would be by sending a verification code to the other location to access the document, another would be to log into the platform, which initially does not send the document if both of the elements do not match any user profile information provided in the platform. If the user is not a registered user, another possibility is to create a new profile, and in the creation process it is easy to check whether the other provided information is correct and in line with the new profiles information. In case of a mismatch of one element, the document cannot be accessed, eliminating the possibility of a data breach. A personal data breach, as defined by Article 4 of the GDPR states:

> "personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed"[91]

As it can be seen, unauthorized disclosure of personal data also constitutes as personal data breach under GDPR and the legal entity whose representative has disclosed personal data is subjected to the procedures laid down in Article 33 "Notification of a personal data breach to the supervisory authority"[92] and notify the supervisory authority unless the personal data

[91] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) , https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN, Article 4(12), Accessed on 20th of May, 2020.

[92] Ibid., Article 33.

breach has not been admitted to be of little significance and it does not interfere with natural person rights and freedom.[93] In many confidential document cases, this scenario could result in disclosure of information that should have not been disclosed.

All in all, Dokobit, by providing the opportunity to only proceed with one element, creates a risk where legal entity representatives, who are natural persons, are at higher risk of unintentional data disclosure. This particularly lowers the trustworthiness of the service provider, as it has not eliminated all the possible risks from their end. There might be a business-related reason present as of why Dokobit has chosen to do so, it could be argued that it might complicate the sending process of the signatory party, as in many cases the personal ID number is not always known. While Dokobit undoubtedly identifies its users and uses QTSP providers in order to provide signing services, the service provider has not fully tackled the issue of weighing out risks in the process of identifying the identity of the other signatory party which receive documents from the sender.

2.4. Electronic identity verification and third party providers

As described before, apart from TS, electronic identity verification is also regulated by eIDAs. eIDAs ensures that electronic identification schemes are to be recognized across borders of the EU, regardless of whether the provider is a QTSP, government institution or a third party provider. An electronic identification scheme has been defined by eIDAs in Article 3(4):

> "'electronic identification scheme' means a system for electronic identification under which electronic identification means are issued to natural or legal persons, or natural persons representing legal persons"[94]

The identification process in itself does not necessarily have to include the use of certificates, as the possibilities are endless depending on the platform and information that is to be accessed.

Third party providers ensure electronic identification as a type of an electronic service. As the name implies – they provide an integration for platforms which promises to identify users in the process of registration or any other action that is carried out in the platform. Many businesses opt for using third party services due to the fact that developing such a scheme on their own is costlier and in order to sustain or ensure a proper identification it requires more resources than a business can handle. For instance, if manual checking of ID's takes place, one must need to employ a department specifically devoted to ID verification. A third party solution integration may be the best option, as third party services which specialize on one specific service most of the times have ensured the highest security as well. Smart ID, for instance, also can be used as an electronic identity verification scheme to authenticate users, however, what is the difference between a QTSP solution, government solution and a solution provided by third parties? Are there any significant differences in personal data protection risks?

---

[93] Ibid.

[94] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN, Accessed on 21st of May, 2020.

2.4.1. Case Study: Gov.UK Verify

A great example is a case study carried out on Gov.UK Verify, which is a United Kingdom's Government initiative towards developing an eGovernment and an eID scheme therein. The eID scheme allows citizens, before the use of government e-services, to verify identity by choosing the favorable way of identification. Gov.UK Verify provides with a survey to determine the most appropriate way for identification and provides with options to choose from. Electronic identification occurs with the help of TS based in UK.

Gov.UK Verify's Data Protection Impact Assessment (DPIA) shows that the personal data protection carried out in the light of this service is based on two legal basis of processing personal data – processing data for tasks carried out in public interest and consent of data subjects.[95] The first one does not raise any questions, however, the latter raises concerns. The DPIA for Gov.UK Verify was carried out prior GDPR, thus raising an issue with the second legal basis, which is consent. Directives 95/46/EC definition on consent "is somewhat cryptic as well as restrictive, as the use of ambiguous terms like "specific", "freely given", and "informed" allow for a broad spectrum of interpretation. Moreover, the Directive says nothing in respect of the methods data controllers may, or should, use as a means of obtaining consent"[96], on contrary,

> "under the GDPR the data subject will be required to express their consent by way of a statement or clear affirmative action. The obvious implication of this being that future consent must be obtained on an 'opt-in' , rather than 'opt-out' , basis if they are to be considered valid. Secondly [..]the GDPR makes it more challenging for data controllers to demonstrate that any consent obtained has been given freely, [..]Thirdly, whilst the DPD fails to provide any details or guidance on the methods that can be used to obtain valid consent, the same cannot be said in respect of the GDPR. As noted above, the GDPR specifically recognizes the validity of several methods that may be utilized by data controllers as a means of obtaining consent, ranging from verbal statements and written statements, to the ticking of boxes and the adjustment of technical settings. In so doing, the GDPR endorses the sentiment that different methods for obtaining consent may be more suitable than others in certain contexts, and compels data controllers to pick those that are most suitably aligned to their data processing practices."[97]

The main concern in this particular case study revolves around the fact whether consent can be considered as valid legal basis for an electronic identity scheme, and this applies to any other services as such. The reasoning behind this concern is that it is not clear on whether the consent is freely given by the data subject as individuals have limited options of such type of e-services to choose from in one Member State and the pressure of society or the government which is rapidly going towards digitization. Specifically – a well-functioning internal eGovernment system might pressure individuals into using these services out of

---

[95] Government Digital Service, GOV.UK Verify
Data Protection Impact Assessment, https://identityassurance.blog.gov.uk/wp-content/uploads/sites/36/2016/05/GOV-UK-Verify-DPIA-v1.0.pdf, p.25., Accessed on 15th of May, 2020.

[96] Sophie Stalla-Bourdillon, Henry Pearce, Niko Tsakalakis, The GDPR: A game changer for electronic identification schemes? The case study of Gov.UK Verify, Institute for Law and the Web (ILAWS), University of Southampton, UK, 2018, p. 792.

[97] Ibid., p. 794-795.

obligation, not out of free will. [98] This particular reasoning can be applied to any other e-service which uses consent as a legal basis of personal data processing. In Gov.UK Verify's case, the DPIA should be redone, as it is outdated and does not comply with GDPR in this matter, however, it is a case to learn from and which raises discussions around consent and the thin line between a freely given consent and the opposite. However, the GDPR challenges with third party providers are not limited to the interpretation of consent.

2.4.2. Case Study: Veriff

One widely known third party electronic identification service is an Estonian developed solution – Veriff. Veriff provides with the opportunity for businesses to integrate their solution in their softwares or platforms for the purposes of identification in the course of registration or carrying out any other action which would require electronic identification.

Veriff is not a TSP, however, is an eIDAS and GDPR compliant electronic identification service. Apart from identification, Veriff provides with the opportunity to monitor results real-time – all the data that have been captured, regardless of whether the verification has been successful or not. The process on how the verification follows is as follows: the user takes a photo of an ID, passport or a drivers' licence, takes a self-portrait and on the other end, Veriff compares the information to the information which is in their data bases on each country documents. The specific information that is extracted from documents is as follows: "portrait photo, name, date of birth, document number, type, issuing country"[99] and data which are only occasionally collected if needed "date of issue, date of expiry, personal number, gender, nationality, citizenship, address"[100]. Veriff does not collect information on tax numbers, place of birth, etc.

Currently, Veriff possesses more than 7,700 government issued document samples for comparison and is available in 190 countries.[101] Veriff also provides with simpler authentication and verification schemes, as for instance, it provides to BLOCKCHAIN, which is a cryptocurrency exchange and Airdrop platform – it does not require a self-portrait or an ID, however, the account and wallet is secured with a sequence of words, PIN and an SMS confirmation. In other words – the authentication and identification method is to be applied appropriately to the respective purposes. For instance, as it is for data subject requests for the provision of information on data that is in the possession of a company. One must be careful not to act against Recital 36 of the GDPR and retain data more than necessary just for the purpose of responding to the requests.

As described above, some e-services which provide with the opportunity to sign with a qualified e-signature, such as Dokobit, work closely with QTSP and retain data about an individual's certificate in order to ensure the legitimacy of the electronic identity and the signature. However, Veriff does not use certificate data in the process of verifying, as well as does not retain any data from QTSP, therefore the level of assurance cannot be regarded to as "high", but nonetheless, Veriff is known to provide services to banking service providers such as Mintos, Transferwise an TFBank. How does Veriff protect their clients against fraudulent

[98] Ibid., p. 799.
[99] Veriff, Which data elements are extracted and verified?, https://support.veriff.com/en/articles/3462567-which-data-elements-are-extracted-and-verified, Accessed on 20th of May, 2020.
[100] Ibid.
[101] Veriff, https://www.veriff.com/product, Accessed on 20th of May, 2020.

activities? Veriff answers the question: "When we carry out a verification, we use face comparison biometrics, both – machine and human; background voice and video detection; hybrid flagging (human and machine), as well as we check document security elements and document validity"[102], and for an additional cost, Veriff provides KYC services by checking sanction lists and for politically exposed persons (PEP).

Veriff is eIDAS compliant, however, it can be seen that large banks do not use third party electronic identification solutions as such for person authentication. Why? Mostly for security purposes by complying to SCA regulation, and due to the fact that QTSP verify the validity of documents in a more secure manner and ensure the highest level of assurance. For instance, as it is in the case of SmartID – it has introduced ID scanning with NFC technology built-in the devices of individuals to read the information stored on the document. Such actions are much more reliable than a manual data comparison with a template or an official copy of a document issued in the respective country.

The fact that Veriff does not use certificates in the verification process is the reason as of why Veriff has been able to expand in so many countries in such a short of time. Certificates differentiate in each country and the integration of each country information would be lengthier than a simple notion on what holograms appear on each country ID or other documents issued in the respective country. Veriff, however, is a comfortable solution for medium and small businesses who do not have the resources to integrate costlier solutions for identification, or do not require such level of authentication. A good example where Veriff could be useful is to respond to data subject requests for information, but only if choosing the appropriate identification method or to meet KYC requirements in identifying sanctioned and PEP.

[102] Veriff, What fraud prevention mechanisms does Veriff have in place?, , https://www.veriff.com/product, Accessed on 20th of May, 2020

3. Comparative analysis on GDPR, eIDAS and PSD2.

Coming to a conclusion where personal data over the years have grown to undertake the value of our modern day 'gold', and taking into account that:

> "As exponential technologies grow; the amount of personal information companies own about online users is growing exponentially too. In fact, according to IBM, 90% of all of the data in the world has been created in the last two years"[103]

and while online identity configuration almost always involves some activity of data processing, it must be noted that online identity can be both – anonymous and comprised with fake attributes or based on real attributes. [104] For instance, accounts created by verifying identity, or services who have integrated trust service provider services or use information from trust service providers on certificates, hold real and certain identity attributes about a person. The validity of attributes is non-negotiable and the identity is linked to a real individual. However, profiles can be created with fake attributes, e.g., fake addresses, pseudonymised usernames in different forums, such as Reddit, or social platforms, like Facebook and Instagram, forming an online identity of a non-existent person. In short, "while all the identity attributes are personal data, personal data is not always an identity attribute"[105]

As it is known that identity theft is one of the greatest risks associated with online identity, even if a company is thought to be fully equipped with dealing with such occurrences, therefore providing with more reasons of one to remain anonymous. Andrew Lewman, executive director of the "Tor Project" adds that he:

> "hopes to re-anonymise the web and that the ability to be anonymous is increasingly important because it gives people control, it lets them be creative, it lets them figure out their identity and explore what they want to do, or to research topics that aren't necessarily 'them' and may not want tied to their real name for perpetuity"[106]

and while online anonymity is important in terms of cybersecurity reasons and also for other reasons, such as Andrew Lweman states. For technological advancement and development, establishing a legitimate and liable online identity is equally crucial.

However, knowing that anonymous personal data are not a subject of GDPR, any other means, such as pseudonymisation, must be taken into consideration in order to strive for the maximum security of personal data, as well as to avoid unnecessary data disclosure where it is not needed. The continuing analysis will be carried out in a way to understand whether the maximum appropriate means have been applied to protect one's data and to eliminate risks of data breach and to understand where eIDAS and PSD2 possibly overlap and clash.

3.1.Comparative analysis on case studies

[103] Ana I. Segovia Domingo / Álvaro Martín Enríquez, Digital Identity: the current state of affairs, BBVA Research, No. 18/01, https://www.bbvaresearch.com/wp-content/uploads/2018/02/Digital-Identity_the-current-state-of-affairs.pdf, p.10., Accessed on 30th of May, 2020.

[104] Ibid.

[105] Ibid.

[106] Aleks Krotoski, The Guardian, Online identity: is authenticity or anonymity more important?,https://www.theguardian.com/technology/2012/apr/19/online-identity-authenticity-anonymity, Accessed on 30th of May, 2020.

For case study analysis, four enterprises different in their nature, however, all concerned with electronic identity and facing privacy issues, were chosen, namely, a trust service – SmartID, electronic service for signing documents – Dokobit, a third party electronic identity verification solution – Veriff and lastly, an eID government scheme – Gov.UK Verify.

All service's functionality was explained and aligned with the compliance of GDPR and how service providers ensure data privacy while offering their solutions which concerned electronic identity or its verification. One of the first observations and comparisons which is to be made is between SmartID and Veriff where both provide electronic identity verification services. SmartID is a trust service, meaning that apart from local identity verification services, SmartID is able to issue certificates in the Baltic states, unlike Veriff, which only is concerned with identity verification solutions. During the Veriff case study, it quickly became apparent that Veriff does not use certificates in the identification process and does not retain information from a TS, as Dokobit does, when permitting the access to the platform, document or allowing to sign the document. Apart from the question on whether Veriff is considered a legitimate means on how to verify one's identity, it also must be looked at how Veriff protects its user data.

For TS it is rather simple – eIDAS lays down strict rules which must be complied with, additionally, in order to become a QTSP and to be presented with the EU Trusted mark, the potential TSP must provide with a conformity assessment report to a conformity assessment body for verification. This process includes complete compliance with the GDPR, as eIDAS lays down the obligation to be compliant with relevant personal data protection regulatory acts.[107] However, third party services, such as Veriff, are not subjected of such strict assessments, creating opportunities for such providers to lack security in the personal data protection area. While a picture of an ID is not considered to be special category data, biometrical data are, and Veriff uses facial identification in the process of identifying a person. Additionally, Veriff allows access to the retained data for businesses which use Veriff for monitoring purposes, which means that Veriff shares all the retained data with online platform administrators and developers. According to Article 9 of GDPR biometric data for the purpose of uniquely identifying a natural person are considered to be special category data.[108] Moreover, according to Article 9 (4), "Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health" [109] meaning that in each Member State services such as verify using biometric data can be subjected to limitations. The question is rather philosophical on whether third party services which provide access to the retained data follow 'data minimisation' principle and whether third party services should share the retained data with businesses who implement such services in their platform verification process.

While technically Veriff claims to be GDPR compliant, and it is so in most of the cases, however, in cases where more serious authentication takes place, there is no assessment

[107] Information Commissioners Office, Becoming a qualified trust service provider, https://ico.org.uk/for-organisations/guide-to-eidas/becoming-a-qualified-trust-service-provider/, Accessed on 1st of June, 2020.
[108] [108] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) , https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN, Article 9, Accessed on 1st of June, 2020.
[109] Ibid., Article 9(4)

body to assess such services which enter the market and deal with data of high importance – data concerning an individual's identity. It could be argued that the application of stricter provisions for such services which deal with special category data, specifically with person's identity, could be the solution for these concerns.

Many FinTech startups and digital banking service providers opt for third party electronic identity verification service providers for business purposes. For instance, widely known digital banking services, namely, Revolut and N26 use third party identification services. This is done simply due to the fact that the integration of verification tools which use the information from certificates, such as SmartID, differ in each country, additionally, even the information which is stored in certificates differs amongst countries. If Revolut or N26 would decide upon using a tool similar to SmartID, it would automatically mean the inability to scale their business in such a fast pace and provide services internationally, due to technical obstacles.

Veriff eliminates this problem, however, it does raises questions on whether stricter data protection implications shouldn't be imposed on such services, similarly as it is for trust services. A stricter data protection compliance regulation, monitoring or creating a system of certification for third party service providers which store special category data and are concerned with identity verification, could provide the necessary level of trust for private service providers to integrate such services more safely and avoid any possible risks of data breach. Banks and FinTech startups are equally liable for choosing the appropriate service for identity verification as it is for identity verification services to comply with GDPR, however, a clear trust mark between such services, as it has been distinguished with Trust Services, is not present, therefore making it harder for businesses to understand which KYC services to implement securely. SmartID is a trust service offering a KYC solution, which in the process of provision is able to demonstrate its secure storage of data and by complying to both – eIDAS and GDPR, ensuring the opportunity to create a liable online identity, the possibility to verify ones' identity and by using appropriate level of security to protect personal data.

The latter services chosen for case study are Dokobit and Gov.UK Verify. Dokobit is a platform which provides with the opportunity to sign documents electronically, while Gov.UK Verify is an identity verification scheme which uses trust service providers for identity verification before using government e-services. After studying the functionality and both service provider compliance to GDPR, it was found that both are not compliant with GDPR in different manners. Gov.UK Verify non-compliance lies in an administrative level, namely, the documentation, wording and the fact that the documents have lost their relevance, therefore not providing with accurate information, while Dokobit's potential risks are rather technical and poses risks to data security.

Gov.UK Verify has yet not updated its data protection policy, approach and DPIA accordingly to the new Regulation. With the introduction of GDPR, the scope of "consent" had changed, and as described in chapter 2.4.1., Gov.UK Verify bases its data processing activities on consent and on the notion of carrying activities in public interest. According to GDPR, the legal ground of data processing, which is consent, must be re-thought, in order to avoid interpretational issues. However, while the non-compliance lies within the wording of legal grounds for processing, it does not raise any particular data breach risks. On the other hand, Dokobit's non-compliance raises risks for data security.

Furthermore, Dokobit is an API based solution, which allows to sign documents with integrated nationally available tools provided by TSP, and as concluded in paragraph 2.3.2.,

Dokobit is challenged with potential personal data protection risk in the document sending process. Unlike in Gov.UK Verify case, this particular aspect may potentially give rise to a more serious breach where unauthorized data disclosure could occur. This particular issue could be solved by ensuring the possibility to send a document by filling out at least two elements, thus making the user experience more complex than before but ensuring that the document has been received by the respective party and all risks have been eliminated.

The case studies clearly show that each of the aforementioned services face challenges in GDPR implementation, liability or personal data protection and security issues arising from the services provided. The balance of identity and security of personal data is thin, but not to say that it is not achievable if implemented accordingly, however, it may be at the cost of business development and rapid expansion across borders.

3.2. The clash of eIDAS, PSD2 and GDPR

The clash of all three regulatory acts is in the nature of their aim – two aiming to establish an online identity, data accessibility and a secure authentication, while the other aims to strive for complete control over personal data and data security.

As described above, the importance of ensuring both are present, however, as the line is thin, it can be challenging to navigate the regulatory duties which are imposed simultaneously. After carrying out case studies it became apparent that almost each of the service providers were challenged by data protection issues while trying to fulfil obligations of establishing electronic identities and providing services therein. The next sub-paragraphs will go more in detail on the legal challenges as of why enterprises struggle with the implementation of these specific relevant acts, if they overlap, and if they do – where?

PSD2 and its aim to foster the development of open banking and eIDAS with the aim of establishing secure online identity – both have raised uncertainties and questions in regards to personal data privacy. The main challenges of implementing both regulatory acts are based on legal uncertainty how GDPR, PSD2 and eIDAS interact in cases where any of the regulatory acts conflict. More than one conflict of laws is present amongst both regulatory acts, however, only a few will be looked at in the following paragraphs in order to get a better understanding of a few concepts and their interaction in regards to data privacy.

3.2.1. Open banking vs. GDPR

One of the main ideas behind PSD2 regulation is the idea of open banking and API banking. As explained in the second part of the work, PSD2 allows banks to transfer data to third party providers (TTPs), thus raising questions on personal data security. While the idea on API banking opens many possibilities for new solutions, encourage innovation and thus growth of the financial industry, making consumer lives easier carrying out payments on the Internet, it also raises tensions between both – GDPR and PSD2 in the context of one protecting data while the other encouraging the access to data. There exist main three issues which can be seen on the surface - compliance with GDPR, party liability on receiving consent and security measures ensured in case of data breach. The question on whether PSD2 and GDPR do not clash must be looked at.

Firstly, PSD2 only refers to Directive 95/46/EC due to the fact that PSD2 was enforced prior GDPR, however, while very vague, the notion to comply with data protection

regulatory acts remains intact. And while both regulatory acts seem different in nature, both have one thing in common – both admit consent as one of the basis of processing personal data. In order for TTPs to gain access to data and facilitate a payment, an explicit consent from the data subject must be obtained. The answer to which party must ensure this is unclear, as well as the scope of the term "consent" in PSD2, as it has not been defined.[110] While both acts hold many similarities in terms of obtaining consent, both also share their differences (see *Annex 2 "'Consent' presented by PSD2 and GDPR: key differences"* for an illustrative comparison), as for instance, while GDPR states that customers must be informed by the opportunity to withdraw consent, PSD2 does not preclude such a notion. Furthermore, while according to GDPR the explicit consent does not expire, according to PSD2 the consent expires automatically. [111] As it is known, fines for non-compliance of data protection rules are significant, therefore leaving banks which strive for innovation in an unpleasant situation. Which one, in case of clash, should be taken into account?

The Dutch Data Protection Authority has given a recommendation on the Implementation Act of PSD2 and addressed this issue by stating that PSD2 is to be considered as *lex specialis* to GDPR, meaning that specific provisions prevail over GDPR provisions when in conflict and concern processing personal data for payment service purposes.[112] However, in some instances the knowledge on the fact that PSD2 could be considered as *lex specialis* to GDPR, there are inconsistencies beyond just the correct application of the law. For instance, PSD2 defines 'sensitive payment data' in Article 4(32) as "'data, including personalized security credentials which can be used to carry out fraud"[113], while GDPR defines 'sensitive personal data' as:

> "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation."[114]

However, as there has been no clear indication given on how to interpret 'sensitive payment data' in the context of both acts, it is advised to seek help at the local data protection authorities bureau. Furthermore, as touched upon earlier, consent raises much more questions than 'sensitive payment data' as it concerns the actual acquisition of data. While PSD2 states that explicit consent must be acquired, both have different approaches to what is meant by 'explicit consent'. GDPR holds more extensive rules within the context of the use of explicit

---

[110] EY, How Banks Can Balance PSD2 and GDPR, https://www.ey.com/en_gl/banking-capital-markets/how-banks-can-balance-gdpr-and-psd2, Accessed on 27th of May, 2020.
[111] Ibid.
[112] Deloitte Legal, PSD2 and GDPR: An awkward match?, https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/legal/deloitte-nl-psd2-and-gdpr-an-awkward-match.pdf, p.2., Accessed on 27th of May, 2020.
[113] DIRECTIVE (EU) 2015/2366 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 201 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366&from=EN, Article 4(32), Accessed on 27th of May, 2020.
[114] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) , https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN, Article 9 (1), Accessed on 27th of May, 2020.

consent as a grounds of data processing, as for instance, the consent must be given freely, specifically, and the TTP should provide that the consent has been obtained as well as the client has been informed of his rights to withdraw consent.[115] In this scenario, considering PSD2 is *lex specialis* and prevails over GDPR puts any TTP and banking service at risk of non-compliance with data protection rules and therefore can be subjected to extensive fines.

Moreover, if GDPR is chosen as the primary regulation to follow, the question of who is liable to obtain the consent arises. Logically, if banks are to be precluded to share client data to third party providers, which, in fact, goes in line with data portability principle of GDPR, the receiving end which acquires the information must ensure complete compliance with GDPR, and thus should also obtain explicit consent from data subjects. However, since banks are the controllers of personal data who determine the purpose of data processing activities, in the scenario where only the TTP has received the consent, it is the banks responsibility to make sure that the request is made on valid basis, or in other words – if the explicit consent indeed has been obtained from the data subject.[116] This would mean identifying the person before proceeding with the payment.

While in practice open banking appears to be a great step forward in terms of financial technology development, the legislation has not yet been adapted for such an environment. Many uncertainties exist on how both PSD2 and GDPR should be approached in this situation. Repeatedly, the question on control over personal data and access to information should be revised – should GDPR provide with exemptions or PSD2 should impose stricter obligations, and where is the line where GDPR starts to hinder innovation?

3.2.2. eIDAS vs. GDPR

Similarly, as with PSD2 Directive, eIDAS and GDPR challenge each other in a similar manner on establishing a clear online identity and data privacy, however, in order to foster the interaction between both, a privacy enhancing technique, called pseudonymisation can be used in order to lessen the data security risks. In short, Pseudonyms are artificial identifiers which are generated to replace personal data or any other information for purposes of hardening the process of identifying a person. A use of such technique complies with the requirement of privacy by design mentioned in GDPR, on the other hand, eIDAS also strives for privacy by design and recognizes pseudonymisation as a tool in Article 5 (2):

> "Without prejudice to the legal effect given to pseudonyms under national law, the use of pseudonyms in electronic transactions shall not be prohibited."[117]

However, while both regulatory acts aim to enhance privacy by design and precludes pseudonymisation, the interpretation of term 'pseudonymisation' under eIDAS and GDPR are different and rather incompatible, which raises legal uncertainty and does not create

---

[115] Deloitte, PSD2 and GDPR – Friend or Foes?, https://www2.deloitte.com/lu/en/pages/banking-and-securities/articles/psd2-gdpr-friends-or-foes.html, p.3. Accessed on 27th of May, 2020.
[116] Ibid., p.2. Accessed on 27th of May, 2020.
[117] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN, Article 5 (2), Accessed on 1st of June, 2020.

consistency in terminology, similarly as it was presented in PSD2 and GDPR on the term 'consent'.

Prior the comparison on the interpretation, it must be noted that Commission Implementing Regulation (EU) 2015/1501 Annex 1 lays down the minimum data set for a natural person, while Annex 2 defines the minimum data set for a legal person. The minimum data set (MDS) for a natural person is defined as follows:

> "The minimum data set for a natural person shall contain all of the following mandatory attributes: (a) current family name(s); (b) current first name(s); (c) date of birth; (d) a unique identifier constructed by the sending Member State in accordance with the technical specifications for the purposes of cross-border identification and which is as persistent as possible in time.
>
> The minimum data set for a natural person may contain one or more of the following additional attributes: (a) first name(s) and family name(s) at birth; (b) place of birth; (c) current address; (d) gender."[118]

As it can be seen, the list comprises of data which are mandatory and optional, as it is known from GDPR, the "data minimization" principle should be applied in the processing of data, therefore, it should be carefully weighted out which data are necessary to carry out certain activities. The mandatory identifiers may vary by Member States, as for instance 'unique identifiers' may differ in each state.

As mentioned above, Article 5 (2) of eIDAS precludes the use of pseudonyms in electronic identification procedure and other electronic transactions, however, while eIDAS refers to the term in the Regulation, eIDAS does not clearly define the word 'pseudonym', the term afterwards is only used in relation to qualified certificates. [119] At first glance, it does appear that eIDAS fosters the use of pseudonyms for data protection purposes in the process of establishing an electronic identity and developing identity verification schemes, as the use of pseudonyms provides with greater protection. Examples for such a use in national eID systems are present, a great example to be seen is in Austria.

> "In Austria, eIDs use a Unique Identifier (UID) that derives from the Central Residents Register. The architecture resembles in some respects Estonia's, which also uses central Resident Numbers. In contrast to Estonia, where Residents Numbers are publicly available information, in Austria it is prohibited by law to share this number with the services. Instead the system employs Sector-specific PINs (ssPin) – pseudonyms constructed partly from citizen number and partly from the services requiring them. This way every department receives different credentials for the same

[118] Commission Implementing Regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015R1501, Annex 1, Accessed on 1st of June, 2020.

[119] Niko Tsakalakis, Sophie Stalla-Bourdillon and Kieron O'Hara, What's in a name: the conflicting views of pseudonymisation under eIDAS and the General Data Protection Regulation, Open Identity Summit 2016, Available at: https://subs.emis.de/LNI/Proceedings/Proceedings264/167.pdf, p.169, Accessed on 1st of June, 2020.

user and the eID is cross-sector unlinkable which does not allow to trace the transactions of a user across the system"[120]

Similarly, Germany's Neuer Personalausweis (nPA), introduced in 2010, also has adopted pseudonyms, since in Germany the central object of the system is eID card. [121] The difference in this eID card that while it is a physical identity card, it also establishes digital identity.[122] This means that the user itself is in control of their eID and there is no Identity Provider present, the user has the right to decide whether, when and where their personal data will be disclosed – when a nPA is used to access a service, a unique pseudonym is generated for the specific session.[123]

Technically, such as in cases of Germany and Austria, it is possible to use pseudonymisation in part of an eID scheme, but it is the combination of eIDAS and GDPR where problems arise. GDPR came into force after eIDAS and simultaneously came along a clear definition of 'pseudonymisation'. Article 4 (5) defines the term as follows: "the processing of personal data in such manner that the personal data can no longer be attributed to a specific data subject without the use of additional information"[124] Furthermore, the additional information, which is included in the definition, must be stored separately by the data controller and by ensuring the appropriate technical security means in order to establish non-attribution.[125] It also has to be noted that only anonymized data are exempt from GDPR, not pseudonymised, as they still fall under the scope of GDPR, even if GDPR admits pseudonymisation is able to reduce risks of data breach. But, as Recital 26 of GDPR states, pseudonymised data are considered still to include information relating to an identifiable natural person if with the use of additional information the pseudonymised data can be attributed to a natural person.[126]

The problem with GDPR's definition is that it poses difficulties to be complied with, if not impossible to be able to meet GDPR's requirements, taking into account the Minimum Data Set (MDS) defined in eIDAS. As clearly stated by GDPR, in order for data to be

---

[120] Ibid.

[121] Signicat, Digital Identity in Germany – market status, trends, and regulations that you need to consider, https://www.signicat.com/resources/digital-identity-in-germany, Accessed on 2nd of June, 2020.

[122] Ibid.

[123] Niko Tsakalakis, Sophie Stalla-Bourdillon and Kieron O'Hara, What's in a name: the conflicting views of pseudonymisation under eIDAS and the General Data Protection Regulation, Open Identity Summit 2016, Available at: https://subs.emis.de/LNI/Proceedings/Proceedings264/167.pdf, p.169, Accessed on 1st of June, 2020.

[124] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) , https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN, Article 4 (5), Accessed on 2nd of June, 2020.

[125] Niko Tsakalakis, Sophie Stalla-Bourdillon and Kieron O'Hara, What's in a name: the conflicting views of pseudonymisation under eIDAS and the General Data Protection Regulation, Open Identity Summit 2016, Available at: https://subs.emis.de/LNI/Proceedings/Proceedings264/167.pdf, p.169, Accessed on 1st of June, 2020.

[126] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) , https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN, Recital 26, Accessed on 2nd of June, 2020.

considered pseudonymised, any attribution of information to a natural person should be excluded. [127] This could be achieved amongst systems which allow for selective disclosure:

> "Selective disclosure allows the system to transmit only those attributes of the eID that are absolutely necessary for the needs of each service, i.e. if a service needs only to know if a user is a citizen or not, the system can reply with only a pseudonym for the particular user and a Yes/No answer to their citizen status"[128]

The issue with this is that the MDS defined in eIDAS fails this test and cannot comply to GDPR standards of 'pseudonymisation' due to the fact that Implementing Regulation 2015/1501 states that it is *mandatory* to *always* include the identifiers named in Annex 1 of the Implementing Regulation to identify an individual. While eIDAS precludes the possibility of pseudonymisation, it is not achievable with the data protection regulation currently at place, therefore pseudonymisation as a tool for ensuring more privacy in eID schemes fails according to GDPR.

Both Regulations clearly do not share the same approach to pseudonymisation – while GDPR presents pseudonymisation as a tool to eliminate data protection risks, eIDAS considers pseudonymisation as a tool which helps to generate more secure Unique Identifyers. "Art 5 of the GDPR provides a waiver of the requirement for a legal basis to process data where, in conjunction with art 6(4), datasets that have been pseudonymised can be further processed if the controller deems the processing 'compatible' with the initial purpose(s)"[129], which could be an issue, if it is assumed that the conditions of the definition are met, due to the fact that many services nationally, which are connected to an eID scheme collect vast amounts of data, as for instance, healthcare providers or tax institutions. Yet, eIDAS has not precluded the use of a plurality of pseudonyms in accordance with the particular service each time. [130]

To conclude, in the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: "Online Platforms and the Digital Single Market - Opportunities and Challenges for Europe", the Commission encourages online platforms to accept eIDs as means to authenticate users, in accordance with eIDAS. [131] However, the opportunity to use systems which are developed in a way of using officially approved national identities to private service providers could raise issues. [132] eIDAS limits pseudonymisation to be as a replacement for Unique Identifiers by not allowing selective disclosure, furthermore, if GDPR considers pseudonymiation as a means of ensuring a higher level of privacy, eIDAS fails to

---

[127] Niko Tsakalakis, Sophie Stalla-Bourdillon and Kieron O'Hara, What's in a name: the conflicting views of pseudonymisation under eIDAS and the General Data Protection Regulation, Open Identity Summit 2016, Available at: https://subs.emis.de/LNI/Proceedings/Proceedings264/167.pdf, p.171, Accessed on 1st of June, 2020.
[128] Ibid.
[129] Ibid.
[130] Ibid.
[131] European Economic and Social Committee, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Online Platforms and the Digital Single Market - Opportunities and Challenges for Europe
[132] Niko Tsakalakis, Sophie Stalla-Bourdillon and Kieron O'Hara, What's in a name: the conflicting views of pseudonymisation under eIDAS and the General Data Protection Regulation, Open Identity Summit 2016, Available at: https://subs.emis.de/LNI/Proceedings/Proceedings264/167.pdf, p.171, Accessed on 1st of June, 2020.

ensure data privacy of users, and is to be considered as a privacy issue if used in commercial online platforms. [133]

[133] Ibid.

4. Conclusion

If one must answer the question of "Does one of the main principles of GDPR to ensure control over personal data conflict with eIDAS Regulation and PSD2 Directive to ensure electronic identification and establish an online identity and whether online anonymity can be achieved? the scope of the answer to this question is dependent on how the term 'online anonymity' is perceived and interpreted.

Given that establishing an online identity always includes processing of personal data which relate to natural persons, and anonymity is ensuring complete anonymity, by not precluding any use of personal data - yes, they conflict in the sense that none of the data processing activities relating to electronic identification services are possible to be anonymized due to the necessary Minimum Data Set required for proper identification and attributes which are needed to ensure identification. However, such a conclusion is rather obvious. Therefore, due to the fact mentioned above and the fact that anonymous data are not subjected to GDPR, 'ensuring online anonymity' throughout this paper was considered as more of a try to ensure personal data protection at the highest level possible, by implementing the necessary technical means to eliminate all risks of personal data exposure, as well as to use all technical measures to limit the amount of personal data being processed, such as complying by the data minimization principle or implementing pseudonymisation as a security tool for personal data.

1. SmartID is GDPR compliant due to strict restrictions and rules laid down by eIDAS for trust service providers. When creating a SmartID account, similarly, as Veriff does with client authentication – an ID card and biometrical data are obtained and stored in their data base. SmartID works as an intermediary between the user and the administrator of the online platform, confirming the identity and afterwards only sending an affirmative or negative answer to the service provider about the user, allowing or not allowing the access to the platform. In contrast, with a third party electronic identity verification integration, such as in the case of Veriff, while Veriff affirms the identity of an individual, it also provides the administrator of the platform with an opportunity to monitor each and single attempt to authenticate, successful authentications and failed ones together by providing access to photos of ID's and facial pictures. The issue with this is that it is unclear if by providing a platform for businesses to manage and store ID cards and biometrical data, does it not pose more risks for data privacy? The answer to this can only be speculated – it may raise concerns on whether the administrator of the platform *needs* to access photos of ID's and facial photos in order to allow the access or carry out the registration process of a platform, as it may not be compliant with the 'data minimization' principle of GDPR.

However, while this particular TPP is considered to be GDPR compliant, it poses more risks by sharing the information about ID documents and photos of individuals than as a TS provider, namely, as SmartID, which does not share this particular information, but rather information on whether the person trying to access the platform is indeed the individual at hand. A solution was proposed in the paper of ensuring a supervisory body or a system of certification which allows to administrate a solution related to KYC and electronic identification processes, as it is with QTSP, in order to avoid risks of not complying with the aforementioned 'data minimization' principle, the aim of ensuring

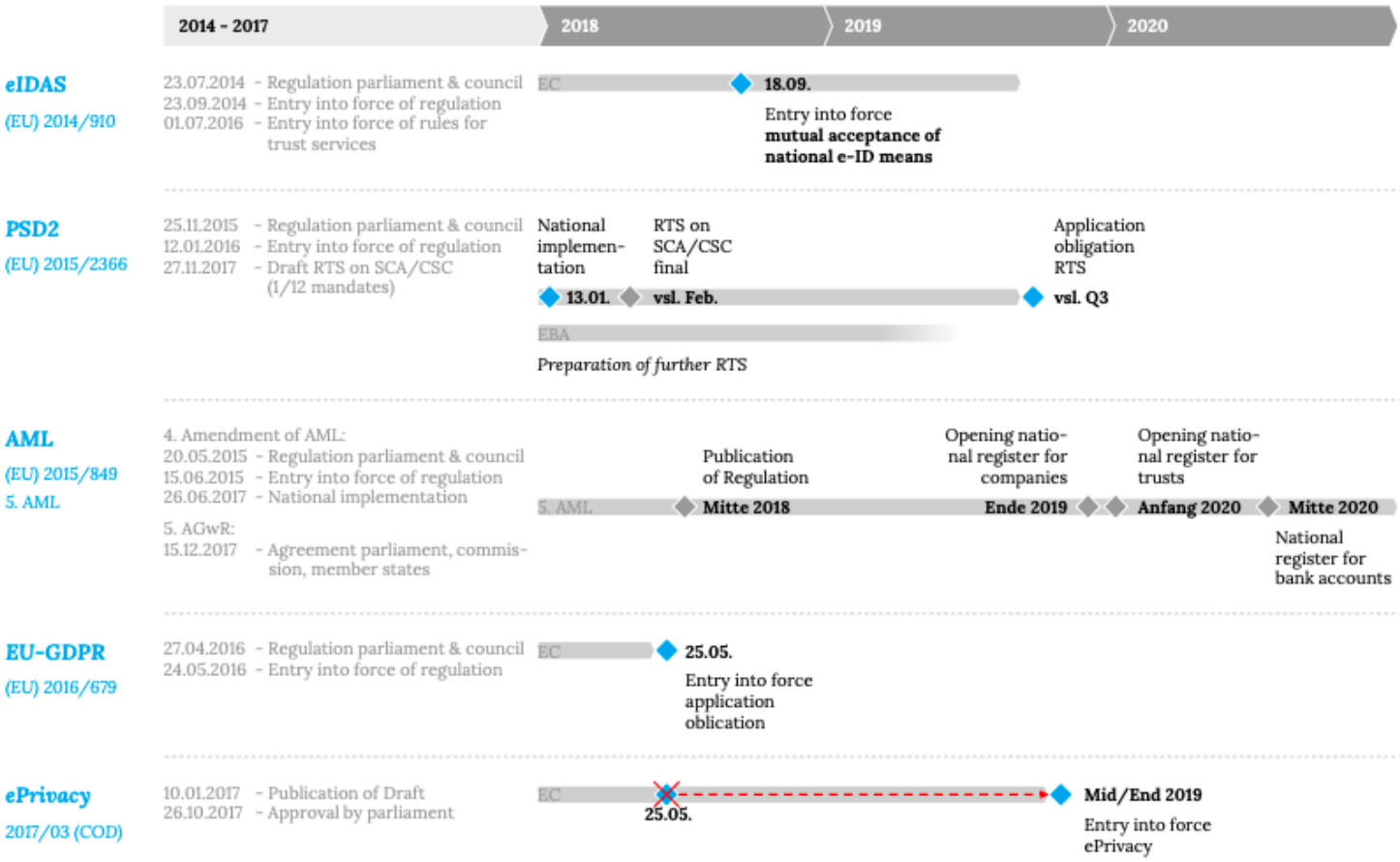
'online anonymity' and, certainly, by failing to ensure the appropriate security measures to protect personal data.

2. The rest of the service providers faced regulatory challenges more than technical, as for instance Gov.UK Verify has not updated their personal data protection related documentation, and the current DPIA has been carried out according to Directive 95/46/EC, which has clear distinctions in defining 'consent' in comparison with GDPR. Dokobit, however, has risks yet to weigh out in terms of allowing to send a document for signing with the opportunity to only provide with one element of identifying the receiver, and it is more a question of a DPIA and the likeliness of such an occurrence than a breach of GDPR. None of the aforementioned case studies grossly breach GDPR, but rather face challenges in ensuring the maximum security and control for which GDPR strives for.
3. During the process of comparing specific requirements between all three regulatory acts, it was found out that all three acts had different interpretation of the same terminology which does not complement each other and thus raising challenges. In the case of PSD2 and GDPR, the elements of which fulfill the requirement of 'consent' vastly differ *(see Annex 2.)*, thus raising uncertainty to which requirements of 'consent' to follow. The Dutch DPA have proposed the PSD2 to be *lex specialis* to GDPR, however, PSD2 does not lay down the necessity to inform customers of the possibility to withdraw consent which is a requirement of GDPR. Therefore, if complying with PSD2 alone, a risk of data protection requirements could be breached. In this particular scenario, in order to avoid breach of GDPR requirements while simultaneously complying with PSD2, it would be advised to implement the requirements which are of stricter nature from both regulatory acts. For instance, if GDPR states to inform the customers of consent withdrawal, while PSD2 does not – it would be advised to inform the customers nevertheless.
4. Moreover, in the case of eIDAS and GDPR, the issue lies between whether 'pseudonymisation' as a concept is achievable in the light of both Regulations, as both use different approach to 'pseudonymisation'. GDPR uses pseudonymisation as a tool of ensuring more privacy and eliminate any risks, while eIDAS only interprets pseudonymisation as a means of ensuring more securely generated Unique Identifiers. The application of pseudonymisation is not achievable in the context of 'pseudonymisation' definition laid down in the GDPR as it is too strict for the fulfillment in accordance with the Minimum Data Set required for electronic identification required by Implementing Regulation 2015/1501.

All in all, each and every case requires an individual approach and risk assessment in order to understand the necessary measures, means and tools to ensure the maximum protection of one's personal data and identity. Does GDPR aim of giving more control over personal data, ensure security and possibly the opportunity to anonymize personal data conflict with the aim of establishing online identity? Yes, however, it is in the hands of providers of such services to ensure the highest level of protection of such sensitive personal data, and a possible supervisory authority which weighing out on whether the data should or should not be shared with third parties, and risks associated with such activities. Furthermore, the regulatory acts must be subjected for revision in order to eliminate the interpretational issues which raise legal uncertainty and challenges.

Annex 1.

Timeline of the European legal framework for digital identities and communication*



**Source: Andrea Müller Asquared, eIDAS, PSD2, GDPR & Co: The European legal framework for digital identities and communication, Available at: https://asquared.company/public/asquared-blog_post_en_2018-02-01_eidas-psd2-gdpr-u-co_v1.pdf, Accessed on 15th of May, 2020.*

Annex 2.

'Consent' presented by PSD2 and GDPR: key differences

Consent element	GDPR	PSD2
Consumer consent to process data must be freely given and for specific purposes		
Customers must be informed of their right to withdraw their consent		
Consent must be explicit in the case of sensitive personal data or trans-border dataflow		
Data processing and sharing is explicitly requested by the customer		
Consent expires automatically		
Consent must be clear, specific and informed		

***Source: EY, Available at: https://www.ey.com/en_gl/banking-capital-markets/how-banks-can-balance-gdpr-and-psd2, Accessed on 27th of May, 2020.*

Bibliography

Primary sources:

1. Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) , https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN;
2. Treaty of Functioning of the European Union, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012E/TXT&from=EN;
3. Charter of Fundamental Rights of the European Union, , https://www.europarl.europa.eu/charter/pdf/text_en.pdf;
4. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995, http://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN,
5. Weltimmo s. r. o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság, Case C230/14, http://curia.europa.eu/juris/document/document.jsf?docid=168944&doclang=EN;
6. Google Spain SL v. AEPD (The DPA) & Mario Costeja Gonzalez, C-131/12, http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&docid=152065 ;
7. Maximillian Schrems v. Data Protection Commissioner, Digital Rights Ireland, C-362/14, http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=23555;
8. Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 201 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366&from=EN;
9. Comission delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R0389&from=EN;
10. Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN,;
11. Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN;
12. European Commission, Payment Services Directive 1 – Directive 2007/64/EC, https://ec.europa.eu/info/law/payment-services-psd-1-directive-2007-64-ec/law-details_en;

13. Commission Implementing Regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015R1501;
14. European Economic and Social Committee, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Online Platforms and the Digital Single Market - Opportunities and Challenges for Europe, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016DC028;
15. European Union Agency For Network And Information Security, Security guidelines on the appropriate use of qualified electronic signatures Guidance for users, December 2016.

Secondary Sources

16. Peter Carey, *Data Protection: Fourth Edition – A Practical Guide to UK and EU Law*, Oxford University press, 2015;
17. Prof. Silvia Parusheva, *Identity Theft and Internet Banking Protection*, University of Economics – Varna, Economic Alternatives, Issue 1, 2009;
18. Jake Stroup, *A Brief History of Identity Theft,* The Balance, Available at: https://www.thebalance.com/a-brief-history-of-identity-theft-1947514;
19. John Stevenson, *All you need to know about Dark web – How to access and what to look out for: How to access and what to look out for* ,Available at: https://books.google.lv/books?id=OAZuDAAAQBAJ&printsec=frontcover&hl=lv#v=onepage&q&f=false;
20. Andrea Müller, *eIDAS, PSD2, GDPR & Co The European legal framework for digital identities and communication*, 2018, Available at: https://asquared.company/public/asquared-blog_post_en_2018-02-01_eidas-psd2-gdpr-u-co_v1.pdf;
21. Marijke De Soete, *eIDAS Regulation – eID and assurance levels – Outcome of eIDAS study*, Security4Biz (Belgium), 24 June 2015; Available at: https://docbox.etsi.org/workshop/2015/201506_securityweek/eidas_thread/s03_eid/security4biz_de_soete.pdf;
22. Mariano Di Martino, Pieter Robyns, Winnie Weyts, Peter Quax Wim Lamott1, and Ken Andries, *Personal Information Leakage by Abusing the GDPR "Right of Access,* Hasselt University, Expertise Centre for Digital Media, Law Faculty, May, 2019;
23. Tamas Szadeczky, *Enhanced functionality brings new privacy and security issues – an analysis of eID*, Masaryk University Journal of Law and Technology;
24. Sophie Stalla-Bourdillon, Henry Pearce, Niko Tsakalakis, *The GDPR: A game changer for electronic identification schemes? The case study of Gov.UK Verify*, Institute for Law and the Web (ILAWS), University of Southampton, UK, 2018, p. 792.
25. Anthony Cuthbertson, *Stolen UK identities selling for a little as £10 on the dark web*, The Independent, https://www.independent.co.uk/life-style/gadgets-and-tech/news/dark-web-id-value-hackers-cyber-crime-a8683821.html
26. Doug Shadel, *Is My Identity on the Dark Web?,* AARP, https://www.aarp.org/money/scams-fraud/info-2018/what-is-the-dark-web.html,

27. DPO, *Summaries of EU Court Decisions Relating to Data Protection 2000-2015*, Data Protection Officer, 2000-2015, Available at: https://ec.europa.eu/anti-fraud/sites/antifraud/files/caselaw_2001_2015_en.pdf;
28. European Union Agency For Network And Information Security, *Qualified Website Authentication Certificates Promoting consumer trust in the website authentication market*, 2015., p.22.
29. Niko Tsakalakis, Sophie Stalla-Bourdillon and Kieron O'Hara, *What's in a name: the conflicting views of pseudonymisation under eIDAS and the General Data Protection Regulation*, Open Identity Summit 2016, Available at: https://subs.emis.de/LNI/Proceedings/Proceedings264/167.pdf;
30. Ana I. Segovia Domingo / Álvaro Martín Enríquez, *Digital Identity: the current state of affairs, BBVA Research, No. 18/01*, Available at: https://www.bbvaresearch.com/wp-content/uploads/2018/02/Digital-Identity_the-current-state-of-affairs.pdf,
31. European Comission, *Protection of personal data*, Available at: https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/know-your-rights/freedoms/protection-personal-data_en,
32. European Data Protection Supervisor, *The history of the General data protection regulation*, Available at: https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en,;
33. EUGDPR, *How Did We Get Here?*, Available at: https://www.eugdpr.org/how-did-we-get-here-.html;
34. Jake Frankenfield, *eIDV (Electronic Identity Verification)*, Investopedia, Available at: https://www.investopedia.com/terms/e/eidv-electronic-identity-verification.asp,
35. Aleks Krotoski, The Guardian, *Online identity: is authenticity or anonymity more important?*, Available at: https://www.theguardian.com/technology/2012/apr/19/online-identity-authenticity-anonymity.
36. European Commission, *eIDAS & 4th Anti-Money Laundering Directive - a short update*, https://ec.europa.eu/futurium/en/content/eidas-and-proposal-amendment-4th-anti-money-laundering-directive;
37. European Union Agency for Cybersecurity, *the Value of Online Personal Data*, https://www.enisa.europa.eu/publications/info-notes/the-value-of-personal-online-data;
38. European Parliament, *Personal data protection*, https://www.europarl.europa.eu/factsheets/en/sheet/157/personal-data-protection;
39. European Commission, *Data protection in the EU*, https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en;
40. Scrive, eIDAS: *Standardising Digital Identity in the EU*, https://www.scrive.com/eidas-electronic-identity-in-the-eu/;
41. SK ID, *SmartID*, https://www.skidsolutions.eu/en/services/smart-id/;
42. European Commission, *What does "grounds of legitimate interest" mean?*, https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/what-does-grounds-legitimate-interest-mean_en;
43. SmartID, https://www.smart-id.com/lv/;
44. Dokobit, https://www.dokobit.com/lv/;
45. Veriff, https://www.veriff.com/product;

46. Veriff, *What fraud prevention mechanisms does Veriff have in place?,*Available at: https://www.veriff.com/product;
47. Transferwise, *PSD2 Explained: What is it and why does it matter?*, Available at: https://transferwise.com/gb/blog/what-is-psd2;
48. Thales, *PSD2 - Double down on security with 2‑factor authentication*, Available at: https://www.thalesgroup.com/en/markets/digital-identity-and-security/banking-payment/digital-banking/psd2/strong-customer-authentication;
49. GCN, *The 4 levels of Authentication in a Mobile World*, Available at: https://gcn.com/Articles/2013/02/12/4-levels-mobile-authentication.aspx;
50. [1] European Commission, *Trust Services*,Available at: https://ec.europa.eu/digital-single-market/en/trust-services,;
51. EY, *How Banks Can Balance PSD2 and GDPR*, Available at: https://www.ey.com/en_gl/banking-capital-markets/how-banks-can-balance-gdpr-and-psd2,
52. Veriff, *Which data elements are extracted and verified?,*Available at: https://support.veriff.com/en/articles/3462567-which-data-elements-are-extracted-and-verified;
53. Government Digital Service, GOV.UK Verify, *Data Protection Impact Assessment*, Available at: https://identityassurance.blog.gov.uk/wp-content/uploads/sites/36/2016/05/GOV-UK-Verify-DPIA-v1.0.pdf;
54. Deloitte Legal, *PSD2 and GDPR: An awkward match?*, Available at: https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/legal/deloitte-nl-psd2-and-gdpr-an-awkward-match.pdf;
55. Deloitte, *PSD2 and GDPR – Friend or Foes?*, Available at: https://www2.deloitte.com/lu/en/pages/banking-and-securities/articles/psd2-gdpr-friends-or-foes.html;
56. Signicat, *Digital Identity in Germany – market status, trends, and regulations that you need to consider*, Available at: https://www.signicat.com/resources/digital-identity-in-germany;
57. Intersoft consulting, *General data protection regulation - consolidated version*, Available at: https://gdpr-info.eu/recitals/no-64/;
58. CIFAS, Available at: https://www.cifas.org.uk/;
59. European Commission, *Trusted list browser*, Available at: https://webgate.ec.europa.eu/tl-browser/#/;
60. European Commission, *Trusted list in Estonia*, https://webgate.ec.europa.eu/tl-browser/#/tl/EE;
61. Information Commissioners Office, *Becoming a qualified trust service provider*, Available at: https://ico.org.uk/for-organisations/guide-to-eidas/becoming-a-qualified-trust-service-provider/;
62. EY Consulting, *How banks can balance GDPR and PSD2*, Available at: https://www.ey.com/en_gl/banking-capital-markets/how-banks-can-balance-gdpr-and-psd2