UNIVERSITY OF TURKU

Right to be Forgotten as a phenomena, European Union and United States approach

Public Law
Faculty of Law
Master's Thesis

Author:
Niklas Ikäheimo

Supervisor:
Prof. Janne Salminen

28.6.2022
Turku

Master's Thesis

Subject: Public Law/ Faculty of Law
Author: Niklas Ikäheimo
Title: Right to be Forgotten as a phenomena, European and United States approach
Supervisor: Prof. Janne Salminen
Number of pages: 77 pages
Date: 28.6.2022

Abstract.

General Data Protection Regulation, known as Regulation (EU) 2016/679 of the European Parliament and of the Council, came to force on May 25, 2018. This regulation aims to modernize and harmonize EU legislation between EU's member states.

Right to be forgotten, in the Article 17 of the GDPR, is right granted to European citizens by the General Data Protection Regulation. This regulation forces companies that want to do business within the EU or with European Citizens to alter their data collection, processing and sharing. Right to be forgotten is a problematic right as it has many limitations, such as public's interest, scientific or historical research, or even statistical purposes.

United States of America, the US, has its own complex legislative system, where each of it's 50 states has their own legislation. Some of them are more strict, such as California with its ”Shine the Light” privacy law and some less strict, such as Wyoming with almost no privacy laws, when it comes to privacy laws, such as GDPR is for the EU.

The sanctions and laws vary in the US between each state, and there is nearly no harmonization on the Federal level, meaning that each state decides on their own how they want to deal with certain areas of law.

Sanctions that a company or organization will receive for failing to fullfil the requirements of the GDPR can reach up to many million Euros. This amount varies on how severe the infringement has

been, and on how big the company at hand is.

Each European member state has had to create their own supervisory authorities to monitor the compliance of companies and organizations and to deal with claims and requests by individuals relating to the GDPR.

Biggest issues of the Right to be forgotten are its limitations and the speed on which information travels these days, also including the fact that when something is put on the internet, it will never be totally removed ever again as someone somewhere might have saved it.

On the US soil, the biggest issue is the non-harmonization of legislation, where basically every state can be seen as individual, and even if companies do obey one states legislation they can be breaking another states legislation at the same time.

The future challenges of the GDPR include the rapid technological development and possible legislation from outside the EU, which may tremple the GDPRs territorial scope.

Key words: EU, Europe, Fines, GDPR, Right to be Forgotten, Right to Erasure, Law, Sanctions, Usa

Table of Contents

REFERENCES

Literature

Anita L. Allen, Unpopular Privacy – What Must We Hide? Part I

Oxford University Press, 2011

Ebook available on: https://play.google.com/store/books/detailsid=91NpAgAAQBAJ&rdid=book91NpAgAAQBAJ&rdot=1&source=gbs_vpt_read&pcampaignid=books_booksearch_viewport

Last accessed 10.2.2022

Anita L. Allen, Unpopular Privacy – What Must We Hide? Part II

Oxford University Press, 2011

Ebook available on: https://play.google.com/store/books/detailsid=91NpAgAAQBAJ&rdid=book91NpAgAAQBAJ&rdot=1&source=gbs_vpt_read&pcampaignid=books_booksearch_viewport

Last accessed 10.2.2022

Muge Fazlioglu, Forget me not: the clash of the right to be forgotten and freedom of expression on the Internet, International Data Privacy Law, Volume 3, Issue 3, 1 August 2013, Pages 149–157

Jussila Jani-Pekka: Reconciling the conflict between the 'immutability' of public and permissionless blockchain technology and the right to erasure under Article 17 of the General Data Protection Regulation, October 2018

https://www.utupub.fi/bitstream/handle/10024/146293/Jussila_Jani-Pekka_opinnayte.pdf?sequence=1&isAllowed=y

Last accessed 10.2.2022

Miriam Kelly, Eoghan Furey and Kevin Curran - How to Achieve Compliance with GDPR Article 17 in a Hybrid Cloud Environment, March 2020

Ebook available on: https://www.mdpi.com/2413-4155/2/2/22

Last accessed 10.2.2022

Maria-Cristina Macocinschi, The right to be forgotten : a conceptual analysis of the right to be forgotten, and its practical implications in the context of search engines, pro gradu, Turku 2015

Nevalainen, Anna-Mari, Digital Privacy in the Transatlantic Networking Society: The Right to Be Forgotten?: Comparative Study between the United States of America and the European Union in Online Privacy Protection Legislation. [Pori]: Turun yliopisto, 2015.

Sanjay Sharma, Data Privacy and GDPR Handbook. Hoboken, 2020.

Ebook available on: http://search.ebscohost.com.ezproxy.utu.fi/login.aspx?direct=true&db=nlebk&AN=2319526&site=ehost-live

Last accesssed 5.2.2022

Giovanni Sartor, The right to be forgotten in the Draft Data Protection Regulation, International Data Privacy Law, Volume 5, Issue 1, 1 February 2015, Pages 64–72

Gutwirth, Serge, Ronald Leenes, and Paul de Hert, Reforming European Data Protection Law. Dordrecht: Springer, 2015.

Santa Slokenberga, Olga Tzortzatou, Jane Reichel, GDPR and Biobanking Individual Rights, Public Interest and Research Regulation across Europe, Springer 2021

Paul Voigt and Axel von dem Bussche, The EU General Data Protection (GDPR) : A practical guide, Cham: Springer, 2017

Ebook available on: EBSCOhost:

http://search.ebscohost.com.ezproxy.utu.fi/login.aspx?direct=true&db=nlebk&AN=1572477&site=ehost-live

Last accessed 12.2.2022

Kruschwitz Udo. Hull Charlie, Searching the Enterprise. Foundations and Trends in Information Retrieval, July 2017

Court cases

The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC, 21st January 2019,

https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc

Last accessed 5.2.2022

GDPR: the Council of State rejects the appeal against the sanction of 50 million euros imposed on Google by the CNIL, June 2020

https://www.conseil-etat.fr/actualites/actualites/rgpd-le-conseil-d-etat-rejette-le-recours-dirige-contre-la-sanction-de-50-millions-d-euros-infligee-a-google-par-la-cnil

Last accessed 10.2.2022

Google Spain SL and Google Inc. V. AEDP & Mario Costeja González

https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62012CJ0131&from=EN

Last accessed 10.2.2022

Melvin V. Reid case review, Feb 28, 1931

https://casetext.com/case/melvin-v-reid

Last accessed 10.2.2022

Sidis v. F-R PUB. Corporation

https://law.justia.com/cases/federal/appellate-courts/F2/113/806/1509377/

Last accessed 10.2.2022

Laws, regulations and official sources

California Consumer Privacy Act of 2018

https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375

Last accessed 5.2.2022

California Legislative Information, S.B. 27, Shine the Light Law of 2003

https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=1798.83.&lawCode=CIV

Last accessed 5.2.2022

Court of Justice of the European Union (CJEU)

https://europa.eu/european-union/about-eu/institutions-bodies/court-justice_en

Last accessed 12.2.2022

The Electronic Communications Privacy Act of California: Senate Bill No. 178, An act to add Chapter 3.6 (commencing with Section 1546) to Title 12 of Part 2 of the Penal Code, relating to privacy. October 8, 2015

https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201520160SB178

5.2.2022

The Electronic Communications Privacy Act of California: Senate Bill No. 178, An act to add Chapter 3.6 (commencing with Section 1546) to Title 12 of Part 2 of the Penal Code, relating to privacy, 1546.4 D. October 8, 2015

https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201520160SB178

5.2.2022

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on theprotection of individuals with regard to the processing of personal data and on the free movement of such data, 1995

GDPR-info, General Data Protection Regulation (GDPR), 2018

https://gdpr-info.eu/

Last accessed 10.2.2022

GDPR-info, General Data Protection Regulation (GDPR)

https://gdpr.eu/tag/gdpr/

Last accessed 10.2.2022

GDPR-info, Art. 4 GDPR - Definitions, 2018

https://gdpr-info.eu/art-4-gdpr/

Last accessed 10.2.2022

GDPR-info, Art. 17 GDPR - Right to erasure (”right to be forgotten”), 2018

https://gdpr-info.eu/art-17-gdpr/

Last accessed: 10.2.2022

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 freemovement of such data, and repealing Directive 95/46/EC. General Data Protection Regulation.

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. Article 4: Definitions

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 freemovement of such data, and repealing Directive 95/46/EC. General Data Protection Regulation., Article 17: Right to Erasure

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 freemovement of such data, and repealing Directive 95/46/EC. General Data Protection Regulation., Article 58, Powers of the Supervisory authorities

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 freemovement of such data, and repealing Directive 95/46/EC. General Data Protection Regulation., Article 83

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 freemovement of such data, and repealing Directive 95/46/EC. General Data Protection Regulation., Article 89. Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

What are the GDPR fines? Two tiers of GDPR fines

https://gdpr.eu/fines/

Last accessed 10.2.2022

Data Protection Officer (DPO), European Data Protection Supervisor

https://edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo_en

Last accessed 10.2.2022

Finnish Police's fine procedure and fines

https://www.poliisi.fi/crimes/fine_procedure

Last accesssed 5.2.2022

Judicial Remedies and Penalties for Violating the Privacy Act, The United States Department of Justice

https://www.justice.gov/jm/eousa-resource-manual-142-judicial-remedies-and-penalties-violating-privacy-act

Last accessed 8.2.2022

Official Statistics of Finland (OSF): Prosecutions, sentences and punishments [e-publication]

http://www.stat.fi/til/syyttr/2019/syyttr_2019_2020-09-24_tie_001_en.html

Last accessed 5.2.2022

Sosiaali- ja terveysministeriön asetus potilasasiakirjoista 298/2009

Available online: https://finlex.fi/fi/laki/alkup/2009/20090298

Last accessed 10.2.2022

Tietosuojavaltuutetun toimisto, Pseudonymised and anonymised data, anonymisation

https://tietosuoja.fi/en/pseudonymised-and-anonymised-data

Last accessed 5.2.2022

Tietosuojavaltuutetun toimisto, Pseudonymised and anonymised data, pseudonymisation

https://tietosuoja.fi/en/pseudonymised-and-anonymised-data

Last accessed 5.2.2022

United States of America's Federal Trade Commission

https://www.ftc.gov/

Last accessed 12.2.2022

United States of America's Federal Trade Commission's Rules and Recommendations

https://www.ftc.gov/enforcement/rules/rules-and-guides

Last accessed 12.2.2022

United States of America's Federal Trade Commission

https://www.ftc.gov/about-ftc

Last accessed 12.2.2022

US Small Business Administration, Privacy Act of 1974

https://www.sba.gov/about-sba/open-government/privacy-act

Last accessed 15.2.2022

Online sources

Apple's iCloud. Apple.com

https://www.apple.com/icloud/

Last accessed 10.2.2022

Rosalie Chan, "The Cambridge Analytica whistleblower explains how the firm used Facebook data to sway elections", Business Insider, May 7, 2020.

https://www.businessinsider.com/cambridge-analytica-whistleblower-christopher-wylie-facebook-data-2019-10?r=US&IR=T

Last accessed 10.2.2022

Jeff Charles. The most effective ways to protect your small business from Cyber attacks. Small Business Trends January 2017

https://smallbiztrends.com/2017/01/how-to-protect-your-small-business-against-a-cyber-attack.html

Last accesssed 6.2.2022

Shoshy Ciment, Macy's tells customers their payment information may have been stolen by hackers. Business Insider November 2019

https://www.businessinsider.com/macys-data-breach-leaked-customer-payment-information-2019-11?r=US&IR=T

Last accesssed 6.2.2022

Data protection under GDPR, European Union – Your Europe, 2021

https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_en.htm

Last accessed 10.2.2022

GDPR Enforcement tracker for fines imposed by the European data protection authorities

https://www.enforcementtracker.com/

Last accessed 8.2.2022

Exchange-rates pound to Euros

https://www.exchange-rates.org/Rate/GBP/EUR

Last accessed 10.2.2022

Alex Hern and Jim Waterson – Sites block users, shut down activities and flood inboxes as GDPR rules loom, The Guardian, May 2018

https://www.theguardian.com/technology/2018/may/24/sites-block-eu-users-before-gdpr-takes-effect

Last accessed 10.2.2022

How to permanently delete something in Windows

https://smallbusiness.chron.com/permanently-delete-something-windows-73434.html

Last accessed 10.2.2022

ICLG: Data Protection Laws and Regulations 2020

https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa

Last accessed 10.2.2022

Legal definition of: Forum Shopping, Merriam-Webster Legal Dictionary

https://www.merriam-webster.com/legal/forum%20shopping

Last accessed 5.2.2022

What are cookies? Kasperky - Cybersecurity company

https://www.kaspersky.com/resource-center/definitions/cookies

Last accessed 8.2.2022

Cameron F. Kerry , Why protecting privacy is a losing game today—and how to change the game. July 2018

https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/

Last accessed 10.2.2022

Silicon Republic. Interview with Ireland's Data Protection Commissioner, Helen Dixon, February 2017

https://www.youtube.com/watch?v=nV7isMbAS7s

Last accessed 6.2.2022

Paul Bischoff. Internet Privacy Laws by State: which US states best protect privacy online?, Comparitech October 23, 2019

https://www.comparitech.com/blog/vpn-privacy/which-us-states-best-protect-online-privacy/

Last accessed 8.2.2022

A Mitchell Polinsky and Steven Shavell - International Review of Law and Economics: Should Employees Be Subject to Fines and Imprisonment Given the Existence of Corporate Liability?

https://www.sciencedirect.com/science/article/abs/pii/0144818893900354?via%3Dihub

Last accessed 10.2.2022

Precendent, Legal Information Institute, Last updated May 2020

https://www.law.cornell.edu/wex/precedent

Last accessed 5.2.2022

Tony Romm and Elizabeth Dwoskin, Facebook is slapped with first fine for Cambridge Analytica scandal, Washington Post, July 11, 2018

https://www.washingtonpost.com/business/economy/2018/07/10/5c63a730-848b-11e8-8f6c-46cb43e3f306_story.html?noredirect=on

Last accessed 10.2.2022

Tankovska H., Facebook's revenue and net income from 2007 to 2020, February 2021

https://www.statista.com/statistics/277229/facebooks-annual-revenue-and-net-income/

Last accessed 10.2.2022

Tietosuojavaltuuten toimisto, Postin rikkeet Euroopan tietosuojalaissa. 18th May 2020

https://tietosuoja.fi/documents/6927448/22406974/Henkil%C3%B6tietojen+k%C3%A4sittelyn+l%C3%A4pin%C3%A4kyvyys+ja+rekister%C3%B6idylle+toimitettavat+tiedot.pdf/b869b7ba-1a05-572e-d97a-9c8a56998fc1/Henkil%C3%B6tietojen+k%C3%A4sittelyn+l%C3%A4pin%C3%A4kyvyys+ja+rekister%C3%B6idylle+toimitettavat+tiedot.pdf

Last accessed 8.2.2022

Vastaamo: Tietomurtoja saattoi olla kaksi..-- Helsingin Sanomat, 2020

https://www.hs.fi/kotimaa/art-2000006698960.html

Last accessed 10.2.2022

Ehkä jopa 32 000 Vastaamon potilaan tiedot ilmestyivät viime yönä Tor-verkkoon – poliisi: "Emme

tiedä, monenko käsissä tietokanta on", Yle Uutiset, January 2021

https://yle.fi/uutiset/3-11757676

Last accessed 10.2.2022

Vastaamo-tapauksesta tehty sata uutta rikosilmoitusta – tietomurto tuli julkisuuteen 4 kuukautta sitten, eikä Sofia, 25, vieläkään tiedä, mitä hänestä netissä kerrotaan, Yle Uutiset, February 2021

https://yle.fi/uutiset/3-11790633

Last accessed 10.2.2022

Davey Winder, 235 Million Instagram, TikTok And YouTube user profiles exposed in Massive Data Leak, Forbes August 2020

https://www.forbes.com/sites/daveywinder/2020/08/19/massive-data-leak235-million-instagram-tiktok-and-youtube-user-profiles-exposed/?sh=172732281111

Last accessed 10.2.2022

5 of the Most Expensive Court Cases in US History, Connorreporting, 2021

https://connorreporting.com/5-expensive-court-cases-us-history/

Last accessed 10.2.2022

ABBREVIATIONS

CJEU	The Court of Justice of the European Union's, established in 1952, main task is to ensure that the European Union's law is interpreted and also applied in the same way in every single of the Member States of the European Union. CJEU can also help national courts by giving them clarification how certain EU law should be interpreted.
CNIL	The Commission nationale de l'informatique et des libertés (CNIL), The National Commission on Informatics and Liberty, in English, is a French administrative regulatory body, that operates independently, but under the French government. Its most important task is to make sure that data privacy laws are applied correctly.
DPC	Data Protection Commissioner is a national independent authority, appointed by the government officials. DPCs are responsible for upholding the fundamental rights of all individuals in the area of the EU to have their personal data protected up to the current standards set out by the General Data Protection Regulations of the EU.
DPO	Data Protection Officer, the primary role of the DPO is to make sure that their organization processes the personal data of its own employees, customers, providers or any of the data subjects' data in compliance with the General Data Protection Regulations.
EU	The European Union, formed with the ”Maastricht” Treaty on European Union in 1993, is an economic and political union between 27 European countries. Its predecessor was the European Economic Community (EEC) which was created by the Treaty of Rome in 1957.

FTC	United States of America's Federal Trade Commission is an independently working US government agency, established in 1914, whose main tasks include promotion of consumer protection, and protecting them from unfair and deceptive practices in the market, and also enforcement of the US civil antitrust laws that are in place.
GDPR	General Data Protection Regulation is a European Parliament and Council Regulation (EU) 2016/679 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 [2016] OJ L119/1. This regulation came to force on May 25, 2018
US	The United States of America is a country mainly located in the continent of North America. The US consists of 50 states. The US was formed by the Declaration of Independence of the United States on July 4th 1776.

INTRODUCTION

When one opens any website for the first time, they will get either a pop up window or a massive alert box including some new General Data Protection Regulation[1], and its rules, telling them that they have to consent to certain collection of personal data before they actually can access the website, these things are called cookies[2] that are being collected about one's visit to the said website. These cookies are then used to track and personalize the advertisements one sees on other websites while browsing the internet.

Most people just hit the concent or accept button right away, but if one checks what data the sites collect they can see way more than what is necessary is being collected, and that's what others just concented to, as the sites also offer possibility to limit the personal data that will be collected during your visit. One is only getting that notification box just because of the new General Data Protection Regulation in the European Union.[3]

The topic of this thesis is Right to be forgotten as a global phenomena, in this introductory part the purpose and goal for the thesis will be states, including the author's hypothesis and research questions. General Data Protection Regulation (hereinafter the GDPR) came to force on May 25, 2018.[4]

The GDPR's main aim is to protect and give more rights to individuals on the internet that has been seen as the new Wild West of the world with little to no regulation. This is done in order to try to regain people's trust that all of their personal information collected is being responsibly treated.[5]

1 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 freemovement of such data, and repealing Directive 95/46/EC. General Data Protection Regulation.

2 What are cookies? Kasperky - Cybersecurity company https://www.kaspersky.com/resource-center/definitions/cookies Last accessed 8.2.2022

3 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 freemovement of such data, and repealing Directive 95/46/EC. General Data Protection Regulation.

4 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 freemovement of such data, and repealing Directive 95/46/EC. General Data Protection Regulation.

5 Paul Voigt and Axel von dem Bussche, The EU General Data Protection (GDPR) : A practical guide, Cham: Springer, 2017

There are fines and penalties imposed on the companies that do not follow the boundaries set by this regulation, and those fines are quite big, reaching up to 20 million Euros.

In a public statement Ireland's own Data Protection Commissioner (hereinafter DPC), Helen Dixon, has clarified that the GDPR does improve the rights of the data subjects by giving them some real control over their own personally identifiable information online. It has to be noted that the GDPR is really clever in its wording as it is seeing into the future with the regulations, as the world and technology around us changes rapidly all the time.

New ways for transparency and notification of GDPR for companies to comply with. The private individuals are in the center and have the power to impact on what information can be stored, shared and in the end they get to deceide what information needs to be removed.[6]

Many of the smaller companies and organizations are only using a small part of the data they have stored over the years and do not even have clear way to search through all their data, meaning that they most likely have no clear understanding of their own stored data, its risks and the value it possesses to others.

The GDPR's Article 17 gives individuals, the data subjects, a legal right by requests to force companies and organizations to remove their personal data even from third party systems and storages which gives the big and small companies many different hard tasks as GDPR regulation covers them all.[7]

This new data regulation forces companies and organizations to reconsider and modify their

---

Ebook available on:
EBSCOhost http://search.ebscohost.com.ezproxy.utu.fi/login.aspx?direct=true&db=nlebk&AN=1572477&site=ehost-live
Last accessed 12.2.2022

6 Silicon Republic. Interview with Ireland's Data Protection Commissioner, Helen Dixon February 2017 https://www.youtube.com/watch?v=nV7isMbAS7s
Last accessed 6.2.2022

7 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 freemovement of such data, and repealing Directive 95/46/EC. General Data Protection Regulation.

management of personal data of the subjects, as before GDPR most of the data storaging and sharing was done automatically and the protection levels of smaller companies were lower as they thought they would have nothing worth stealing, which on the other hand made them an easier target.[8]

Now that personal information is worth millions, even if just in fines, it is really worth protecting that, as not having decent protection measures can account a company to a huge fine under the GDPR, as it means the company has not taken all the necessary means to protect their European clients' personal data.

Simply said any company that takes payments for services online has information worth stealing for the right person, as that payment includes the payment information of the buyer and these leaks of personal information are quite common, even only few make it to the headlines by being massive leaks of personal information including, for example, ones payment information, telephone number and home address.[9]

Companies and organizations are doing their best to keep these leaks secret and under control as it can be massive hit for their income if people using their services lose their trust on the payment or login system a certain company has. Even though services such as Instagram, Youtube and TikTok rarely have anything related to payment information there is still a vast amount of personal information stored in all of these services when people use them, and a breach due to a poor security methods used is not as uncommon as people think it is.[10]

As all of these companies mentioned are being operated by multi billion companies worldwide, so

8 Jeff Charles, The most effective ways to protect your small business from Cyber attacks. Small Business Trends January 2017
https://smallbiztrends.com/2017/01/how-to-protect-your-small-business-against-a-cyber-attack.html
Last accesssed 6.2.2022

9 Shoshy Ciment, Macy's tells customers their payment information may have been stolen by hackers. Business Insider November 2019
https://www.businessinsider.com/macys-data-breach-leaked-customer-payment-information-2019-11?r=US&IR=T
Last accesssed 6.2.2022

10 Davey Winder, 235 Million Instagram, TikTok And YouTube user profiles exposed in Massive Data Leak, Forbes August 2020
https://www.forbes.com/sites/daveywinder/2020/08/19/massive-data-leak235-million-instagram-tiktok-and-youtube-user-profiles-exposed/?sh=172732281111
Last accessed 10.2.2022

one would think that they also have great, if not perfect, security systems on place, but that's not the case as there always is someone who finds a way to breach any protection, and it costs money to create a security system or hire someone else to do it for you or use external company, that specifies in data protection, for that.[11]

Most of the companies and organizations are doing their best to prevent any data leaks or breaches because of the fines GDPR will enforce on companies that do not do so. Starting from 10 Million Euros and going even higher depending on the company's worldwide annual turnover from the preceding financial year, meaning even the biggest companies will do something in order to avoid 2% or 4% of that annual revenue to be given as a fine for them.[12]

The fact that the fines are so high creates also companies and organizations to work on go arounds or bypasses to be able to avoid the need to follow all of the GDPR regulations. Companies have even set out affiliates that work separately from the main company, in case something goes wrong with the GDPR, and the fine is too much, making it possible just bankrupt that affiliate and use another one.

A good example is geo-blocking the possible customers if they are European residents, meaning that they live in the European union, yet allowing the service to be used by third party website by European residents, so that only the third party has to operate within the GDPR's regime and all its regulations and rulings.[13]

1. General Data Protection Regulation and the Right to be Forgotten

11 Santa Slokenberga, Olga Tzortzatou, Jane Reichel: GDPR and Biobanking Individual Rights, Public Interest and Research Regulation across Europe, Springer 2021

12 What are the GDPR fines? Two tiers of GDPR fines
https://gdpr.eu/fines/
Last accessed 5.2.2022

13 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 freemovement of such data, and repealing Directive 95/46/EC. General Data Protection Regulation.

General Data Protection Regulation, also known as Regulation 2016/679 of the European Parliament and Council, is legislative act by the European Parliament and the Council of the European Union.[14] The regulation is an act to help in protecting of natural persons, that are currently residing in the area of the EU, and their rights with a regard to the processing of their personal data and over the movement of such sensible data.

This regulation also repeals the Directive 95/46/EC[15]. The GDPR came to force on May 25, 2018, it is aimed to be the better and more modernized version of the old directive that it repealed as the world has become more focused on the internet, on which the information spreads faster than it ever has spread in any other way before, and it does not matter whether the information is correct or false it still will spread.

GDPR automatically became enforced as a law in each of the EU member state without the need for countries to implement it. It is aiming to modernize and harmonize the area of data privacy laws between all of the Member States and it also introduced a legal framework for us to improve the enforcement and reducting the capita needed to do so for organisations, in hopes of encouraging more economics to grow all around the Europe while giving some feeling of safety online for the end users, as in private persons.[16]

The need for GDPR and its various new articles providing safeguard mechanisms for people has been on the rise lately as more and more big and small companies have misused the information they have collected from people over the years, and so far without any real threat of receiving sanctions.

These news over misuses of stored information and breaches of data, which have received a lot of

14 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 freemovement of such data, and repealing Directive 95/46/EC. General Data Protection Regulation.

15 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 freemovement of such data, and repealing Directive 95/46/EC. General Data Protection Regulation. Repealing Directive 95/46/EC

16 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 freemovement of such data, and repealing Directive 95/46/EC. General Data Protection Regulation.

attention in the media worldwide, alongside with the GDPR have all together raised the awareness of individuals over their own rights on the internet and over the data that will be collected from them.[17] People are also getting more aware of how the collected information is being used by the processors.

As the data is being collected, saved, processed and analyzed for many different reasons by all of these organizations and companies, either big or small, therefore the strict way of handling such data by GDPR,[18] and any further regulation for the internet is the right way to go. All that the companies and organizations do regarding to data is central to their operations in their business models these days. The employees, affiliates and all customers' data saved, or processed, is in the scope of GDPR.[19]

The internet on the other hand has became a playground for the largest of the companies, including Amazon, Facebook, and Google, for example. They mostly just collect and process the data to give their users more personalized possibility to use their services, but at the same time they might want to sell one's information to another company so that their ads will be more targeted towards this individual.

These large companies, however, have had to adapt their habits in order to avoid the fines and sanctions laid out by the GDPR. For example, Google already have adjusted their collection of data, by adding certain information to their user agreement, that one has to accept before being able to use Google's service. This was done briefly after Google received a 50 million Euros fine from the EU for violation of the GDPR.[20]

17 Jussila Jani-Pekka: Reconciling the conflict between the 'immutability' of public and permissionless blockchain technology and the right to erasure under Article 17 of the General Data Protection Regulation, October 2018
https://www.utupub.fi/bitstream/handle/10024/146293/Jussila_Jani-Pekka_opinnayte.pdf?sequence=1&isAllowed=y
Last accessed 10.2.2022

18 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 freemovement of such data, and repealing Directive 95/46/EC. General Data Protection Regulation.

19 Sanjay Sharma, Data Privacy and GDPR Handbook. Hoboken, 2020.
Ebook available on: http://search.ebscohost.com.ezproxy.utu.fi/login.aspx?direct=true&db=nlebk&AN=2319526&site=ehost-live
Last accesssed 5.2.2022

20 The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC, 21st January 2019,
https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc
Last accessed 5.2.2022

This was the case in the Facebook-Cambridge Analytica scandal following the US Presidential elections of 2016, where Cambridge Analytica had used personal data from Facebook's collected data[21] in order sway the US Presidential elections and tried make people vote for Ted Cruz, with the use of personalized and targeted ads for each individual simply based on their behavior and search history.

For example, the Information Commissioner's Office, in the United Kingdom (hereinafter UK), announced in April 2018 it will impose a fine of £500,000 on Facebook over the scandal, as that was the highest possible fine they may give.[22]

At the time of receiving the fine, in 2018, Facebooks paid taxes around 1% of their sales in the UK, and that amount for £15,8 million, while their sales were £1,3 billion in the UK alone. Given that Facebook received a fine for 0,04% of their sales, it wasn't really balanced amount as a fine as they most likely made way more from just selling the information to Cambridge Analytica.

If GDPR had been enforced already by the time that personal data sale scandal happened, as it involved European Residents aswell[23], the amount of fines Facebook would have faced in the EU alone would have been around £1,7 billion, which means around 1,9 billion in Euros.[24] as Facebooks annual revenue from 2017 was over 55 billion US dollars[25],

---

21 Rosalie Chan, "The Cambridge Analytica whistleblower explains how the firm used Facebook data to sway elections", Business Insider, May 7, 2020.
https://www.businessinsider.com/cambridge-analytica-whistleblower-christopher-wylie-facebook-data-2019-10?r=US&IR=T
Last accessed 10.2.2022

22 Tony Romm and Elizabeth Dwoskin, Facebook is slapped with first fine for Cambridge Analytica scandal, Washington Post, July 11, 2018
https://www.washingtonpost.com/business/economy/2018/07/10/5c63a730-848b-11e8-8f6c-46cb43e3f306_story.html?noredirect=on
Last accessed 10.2.2022

23 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 freemovement of such data, and repealing Directive 95/46/EC. General Data Protection Regulation.

24 Exchange-rates pound to Euros
https://www.exchange-rates.org/Rate/GBP/EUR
Last accessed 10.2.2022

25 Tankovska H., Facebook's revenue and net income from 2007 to 2020, February 2021
https://www.statista.com/statistics/277229/facebooks-annual-revenue-and-net-income/
Last accessed 10.2.2022

That fine, as there is no prison sentence possible, would have been sufficient enough to actually make Facebook's CEO Mark Zuckerberg and his team to think more about whether they sell information without permission of the individuals using their online services that do collect personal data from users.

GDPR can be applied world wide to any organisation or company that either does collect, store, process or monitor an European residents' personally identifiable data. The nationality or location does not matter. It also includes the goods and services that are free.[26]

This covers both digitalized form of data and hard copy data. Under the GDPR these data protection authorities do indeed have the powers to impose variety of sanctions with possible negative publicity and could also impose fines with significant amounts. Compensations may also have be payed to individuals who have their rights breached under the GDPR.

The GDPR introduces new terrms and roles for people, companies or organizations all around the world, as GDPR is globally applicaple due to its wording. Most important of these terms to know and understand are Data subject, Data controller, Data processor and Data Protection Officer (hereinafter DPO)[27].

Data subject is always a natural living person who could be identified either directly or indirectly from the collected data, in particular by reference to a personal identifier including the following: their name, an identification number, an online identifier, data of their location, or to one or even more factors specific to the physical, economical, physiological, mental, genetical, cultural or social identity of the person in matter. Anybody residing in the European Union, not just EU citizens, can

26 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 freemovement of such data, and repealing Directive 95/46/EC. General Data Protection Regulation.

27 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 freemovement of such data, and repealing Directive 95/46/EC. General Data Protection Regulation. Article 37: Designation of the data protection Officer, 2018

be considered as data subjects and have their rights protected under the GDPR regime.[28]

The organisation that collects, processes and stores the personally identifiable information (hereinafter PII) is the data controller, and it must, if needed, to fully demonstrate that they are complying with GDPR, meaning that they have to prove they are doing it the right way.[29]

Data processor is a company or an organisation that processes necessary data as they have been instructed by the data controller, as an example cloud host service providers. GDPR is recognising the complicated nature of today's data processing situations and it also identifies that these data processors play an essential part in protecting of all of this data from these European citizens and so it has introduced really direct rules for them, including the record keeping and need for reports over any possible data infringements.[30]

Any person working as a DPO, must have acquired special set of skills, knowledge and expertise of the GDPR and its compliance. This is needed to ensure that the requirements are well known starting from the top level of the management. The DPOs are the point of contact for these national supervisory authorities and they monitor the organization’s compliance level with the GDPR.

The choice is on the organization as a DPO can either be a hired employee of the company or a service that has been outsourced to another organization specialized in providing knowledge of the GDPR. Also a significant limitation on who can be the do is that the DPO cannot be in a controlling position, such as head of human resources, in the company.[31]

---

28 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 freemovement of such data, and repealing Directive 95/46/EC. General Data Protection Regulation.

29 Art. 4 GDPR - Definitions, 2018
https://gdpr-info.eu/art-4-gdpr/
Last accessed 10.2.2022

30 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 freemovement of such data, and repealing Directive 95/46/EC. General Data Protection Regulation. Article 4: Definitions

31 Data Protection Officer (DPO), European Data Protection Supervisor
https://edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo_en
Last accessed 10.2.2022

Under the GDPR it is obligatory for all organizations and companies to appoint a DPO, however, the small companies and organisations which employ less than 250 people are excluded from the requirement of having a DPO.[32]

The right to be forgotten, also known as the right to erasure is the 17th Artice of the GDPR[33], it has been a somewhat debated right under the European Union's General Data Protection Regulation, as it allows one to almost completely request the removal of information regarding to them from any online sources. Whether that information is correct or false plays nearly no role when it comes to the use of this right. Right to be forgotten can be used right as a right but, however, it could also be quite easily abused.

Abusing this right can be done by requesting the removing information that could be necessary for others to know about a company or a person, as the owner of the company could request information over their company to be removed under the Article 17 of the GDPR[34].

Shady acts of past such as frauds, scams or similar can be requested to be removed from online sources, meaning that the information becomes incredibly hard to find, and will not be available by a simple search on the internet, instead people would really have to dig deeper to find that information or even smaller pieces of the information that was requested to be removed from being available online.

As was the case with Mario Costeja Gonzalez, he had done something almost twenty years ago, and that ghost of past was still following him. He is a prime example of someone who would be better off if some information relating to their past was not available.

---

32 General Data Protection Regulation (GDPR), 2018
https://gdpr-info.eu/
Last accessed 10.2.2022

33 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 freemovement of such data, and repealing Directive 95/46/EC. General Data Protection Regulation. Article 17: Right to erasure ”Right to be forgotten”

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 freemovement of such data, and repealing Directive 95/46/EC. General Data Protection Regulation.

Mario Costeja Gonzalez had his house sold on a foreclosure auction and the information resurfaced on the internet as La Vanguardia, a spanish news paper, decided to copy all their old and new published news papers online. As he worked on a area of business where people tend to use Google to see what one has done before this caused him to lose possible clients. [35]

Under the GDPR and its Article 17, Right to Erasure, one can request anything related their personal information to be removed from the internet to certain extend, this can be done to protect your own identity, or it can be done to make certain harmful information concerning the person to disappear from the internet.[36]

Crimes, convictions, accusations are no exceptions to the so called harmful information that can be requested to be removed from the stored data from all over the internet.[37] The limitations, however, does apply if this information required to be removed has public, statistical or historical value to others.

35 Google Spain SL and Google Inc. V. AEDP & Mario Costeja González
https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62012CJ0131&from=EN
Last accessed 10.2.2022

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 freemovement of such data, and repealing Directive 95/46/EC. General Data Protection Regulation. Article 17: Right to erasure ”Right to be forgotten”

37 GDPR-info, Art. 17 GDPR - Right to erasure (”right to be forgotten”), 2018
https://gdpr-info.eu/art-17-gdpr/
Last accessed: 10.2.2022

1.1 Right to be Forgotten in the EU

In the GDPR Right to be forgotten is laid out in the Article 17. The article specifies on when it is possible to have ones information to be removed from the database of a certain company or organization. The article also has some exceptions in the GDPR on when it can be enforced.[38]

The right to be forgotten can also be applied to companies or organizations operating from outside the EU, as long as the subject of the data is living in the European Union. This means that every company in the world is somewhat forced to follow the GDPR if they wish to do business with someone residing in the EU.

The Article 17 of General Data Protection Regulation is covering the following areas. Data subjects have the right to request for an erasure of personal data concerning them without any unnecessary delay and the controller of this data has to erase personal data without delay if certain criteria is met with the data.[39]

Such personal data that is no longer necessary in the relation to the purposes for which they were collected or otherwise processed, or the data subject withdraws consent on which the processing is based and if there is no other legal ground for the processing of this data.If the data subject objects to the processing of their data and there can be found no other legitimate grounds for the processing, or if the data subject objects to the processing pursuant to Article 21, Right to object. All of these datas has to be deleted by the controller.[40]

Any personal data that has been illegally processed, then the personal data has to be erased to

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 freemovement of such data, and repealing Directive 95/46/EC. General Data Protection Regulation. Article 17: Right to erasure ”Right to be forgotten”

39 GDPR-info, Art. 17 GDPR - Right to erasure (”right to be forgotten”), 2018
https://gdpr-info.eu/art-17-gdpr/
Last accessed: 10.2.2022

40 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 freemovement of such data, and repealing Directive 95/46/EC. General Data Protection Regulation. Article 17: Right to erasure ”Right to be forgotten”

comply with the legal obligations under European Union or Member State law to which the controller is actually subjected to, or the personal data that has been collected in relation to the information society services referred to in GDPR's Article 8, which covers child's consent to their information data collection.[41]

If the data controller has made the personal data public, it is forced to erase the personal data. The controller, while taking account of available technology and the cost of implementations, must take only reasonable steps, including the technical measures, to inform other controllers which are processing this same personal data that the subject has requested for the erasure of their data under GDPR.[42]

Limitations should not be applied to the extent that processing is necessary for exercising the right of freedom of expression and information, or for compliance with a legal obligation which requires processing of the data under EU or Member State law to which the controller is subject to or for the performance of a task carried out in the public interest or in the exercise of official authorities power granted for the controller. Personal data can also be kept by the controllers for public interest in the area of public health, and for archiving purposes in the same public interest, scientific or for historical research, or even statistical purposes, or for the establishment, defence or exercise of any legal claims.[43]

This regulation is seen as the toughest and most complex privacy and security law in the whole world, as it imposes obligations to companies all around the world, as long as they aim to or collect data relating to the people in the area of the European Union (hereinafter the EU)[44]. The GDPR has harsh fines against the companies which infringe against its privacy or security standards, with the

41 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 freemovement of such data, and repealing Directive 95/46/EC. General Data Protection Regulation., Article 17. Right to erasure ”Right to be forgotten”

42 GDPR-info, Art. 17 GDPR - Right to erasure (”right to be forgotten”), 2018
https://gdpr-info.eu/art-17-gdpr/
Last accessed: 10.2.2022

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 freemovement of such data, and repealing Directive 95/46/EC. General Data Protection Regulation. Article 17. Right to erasure ”Right to be forgotten”

44 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 freemovement of such data, and repealing Directive 95/46/EC. General Data Protection Regulation.

sanctions reaching up to millions of euros, and actually in some cases even higher, all depending on the severity of the breach and taking also into account the company's revenue.

Right to be forgotten sparked to become used as a right after the Court of Justice of the European Union[45] (hereinafter the CJEU) made its judgement on the case Google Spain SL and Google Inc. v. AEDP and Mario Costeja González[46]. It is the most significant judicial decision regarding the right to be forgotten and it dates back to May 2014.

In its decision the CJEU ruled that Google Spain, meaning Google, was obligated by EU law to delete from its results of searches links to two different newspaper articles that were relating to old information concerning an old foreclosure auction of a real estate of González.[47]

The case on its own and especially its judgment was essential as interpretation of and an application of Directive 95/46/EC, which is also known as the Data Protection Directive that was issued by the European Parliament and the Council of the European Union already back in 1995[48], almost 20 years prior to the case itself.

For the balance of the GDPR enforcement and the requirements by the companies it has to be considered that it is nearly impossible to totally enforce the right to be forgotten as data can be stored away of the control or reach of a company trying to do their best in complying with the the data removal request from an individual.

The use of phones with millions of features, which allows a person to take photos or a screenshot of personal information and distributing these to many other locations by a simple click while using people's private email, or carryable devices, such as USB-drives. Another thing to consider is that deleted files are not fully erased as they may still be on the hard drive, even after emptying the

45 Court of Justice of the European Union (CJEU)
https://europa.eu/european-union/about-eu/institutions-bodies/court-justice_en
Last accessed 12.2.2022

46 Google Spain SL and Google Inc. V. AEDP & Mario Costeja González
https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62012CJ0131&from=EN
Last accessed 10.2.2022

47 Google Spain SL and Google Inc. V. AEDP & Mario Costeja González
https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62012CJ0131&from=EN
Last accessed 10.2.2022

48 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

computers recycle bin, meaning that the personal data can be recovered by other means.[49]

It is nearly impossible to delete just one piece of personal information without having impact on the other data saved, meaning it may not be possible to destroy one's information fully without affecting other necessary data that may still be required by the company or organization, as true deletation of certain files might require the computers or data centers to be wiped totally.

Even if a computer's files are deleten, the most skilled computer technicans can still recover the data, as if something once existed there's always a way to find it again, unless the hard-drives are physically destroyed. Of course organizations can take and many already have taken pre-emptitive measures, such as high level of encryption or limiting the access levels of people who may access certain information, to make this insanely hard and minimizing the risks of data leaks when deleting their files.[50]

As personal information of clients and customers can be saved and processed in many different forms and locations, either locally on a single computer or in a cloud saving system, such as Apple's iCloud[51] or Window's OneSync, or on a certain third party website database, meaning that the information is scattered all around. A safe search tool for simultaneosly looking from all these possible saving locations is required to efficiently and reliably find and erase information if need be, a kind of enterprise search tool.[52]

By implementing and complying with the recommendations, and of course the requests, of the Article 17 of GDPR, the Right to Erasure, into a smaller company's data saving structure, and then receiving a removal request from a subject of their data for the deletation of some data, the organization would have to identify securely, then locate and access the location of the personally

49 Recover lost or deleted files guide, Microsoft 2020
https://support.microsoft.com/en-us/help/17119/windows-7-recover-lost-deleted-files
Last accesssed 10.2.2022

50 How to permanently delete something in Windows
https://smallbusiness.chron.com/permanently-delete-something-windows-73434.html
Last accessed 10.2.2022

51 Apple's iCloud. Apple.com
https://www.apple.com/icloud/
Last accessed 10.2.2022

52 Kruschwitz Udo, Hull Charlie: Searching the Enterprise. Foundations and Trends in Information Retrieval, July 2017

identifiable information and then finally delete it.[53]

The person who is responsible for the erasure of data would mostly likely have to manually log on to each device the organization has been using by using their encrypted login credentials, then they would have to execute only necessary scripts on each of devices used to identify, locate and to fetch the position of any applicable personally identifiable information and finally delete all that information in order to fully comply with GDPR.[54]

To furthermore limit the possibility of information leaks these organizations and companies should consider that the amount of people who have access to the information creates greater risk of a possible data leak. For a organizations or company to limit their risks it could be done by having as minimal amount of people with access to their client's personal information, for example, a team only dedicated in working with the personal data center.

Due to the fact that if everyone has access to the personal information of clients, there is higher chance of someone misusing the information they are able to obtain, meaning that limiting the possibilities of personal information leaks minimizes the risks of having to delete certain information.

Limiting the possible people who can access to the information also makes it easier to track down the one who has misused the information, if compared to a setup where everyone in the company has this possibility to see all the information. Of course people who work closely with the client should have this access, but people working on different parts of the company or organization may be should not have this access.

Not all companies can make a distinction between who has access to the information as everyone

53 Miriam Kelly, Eoghan Furey and Kevin Curran - How to Achieve Compliance with GDPR Article 17 in a Hybrid Cloud Environment, March 2020
https://www.mdpi.com/2413-4155/2/2/22
Last accessed 10.2.2022

54 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 freemovement of such data, and repealing Directive 95/46/EC. General Data Protection Regulation. Article 17. Right to erasure ”Right to be forgotten”

works with everything within the company. If this is the case then it comes down to the tracking of the company's own employees so that they cannot misuse the information that they do have access to.

Lets take for example, a hypotethical company or organization that creates and upholds mobile phone applications for bigger companies who do provide their services through this mobile phone application, and they operate within the EU with EU citizens as their customers. This application has a limited personel with access to the data that the applications do collect. This company that creates and upholds the application has an employee with access to the data, who then uses this information for their own amusement.

The information is then being leaked to a third party, for example a friend group of this employee, without a consent received from their data subjects. This is later found out by the authorities as an user of the mobile application makes a claim that their personal information has been leaked from this application and wishes it to be removed from the application and its third parties data bases as they do not trust their information to be safe with them, and these leaks of the information has been harmful to them.[55]

When this misuse of data comes to the guilty party, it is still the company or organization as it is their employee who has misused the information they have had access to and under the GDPR the company is seen as the responsible party for the actions of their employees, and they are the one who will have to deal with the high fines embodied in the GDPR.[56]

Another possible scenario with the same two hypotethical companies is that the user of the mobile application infroms the authorities of the possible misuse of the information by the company that offers its services through the mobile application. The authorities will have an investigation over this company and find the breach, but instead of the company who created the application they issue

55 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 freemovement of such data, and repealing Directive 95/46/EC. General Data Protection Regulation., Article 17. Right to erasure ”Right to be forgotten”

56 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 freemovement of such data, and repealing Directive 95/46/EC. General Data Protection Regulation.

the fines for the company providing services through the mobile application, as they are responsible, to some extend, for their users data to be kept safe.[57]

The company has the possibility depending on how their contract is with the mobile application to either try to take the fine and fight it in court against the EU, or take it to court and blame the data misuse on the company that created the application, as in the end they are the ones employeeing the person who was in charge of the misuse of information and made the data leak possible.

These court cases both are really complicated and come down to the fine print of both the application end user license agreement, and the contract between the company creating and upholding the mobile phone application and the company providing services through this application.

Most of us do no really care what personal data an organization or a company has about them, as often it is just their name, phone number, e-mail and their IP-address or physical address where they live, which can all be found out via multiple other ways than from a specific company or organization.

However, if a company or an organization collects more sensitive personal information about their clients, which indeed is the case in medical centers and organizations working with people's health, the amount of people who might request their information to be permanently removed, under the GDPR's Right to be forgotten[58], just in case will be higher as people don't want certain sensitive information about their past leaked under any circumstances.

There's also the factor of what information might be required by the authorities to be kept by the companies, enforced by a certain country, and thus cannot be deleted even by a request from an individual. A good example is the Finnish regulation regarding medical patient records, Degree of

57 General Data Protection Regulation of the European Union
https://gdpr.eu/tag/gdpr/
Last accessed 5.2.2022

58 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 freemovement of such data, and repealing Directive 95/46/EC. General Data Protection Regulation.

Ministry of Social Affairs and Health on patient records 298/2009, which requires companies to keep the medical records of their patients for further use by the Finnish authorities.[59]

A Finnish psychotherapy center called Vastaamo, which was used by many Finnish celebrities and other people, was recently discovered to have had it's clients sensitive personal data to be hacked between the years 2018-2019. The job that the people working in Vastaamo do includes, for example discussing and helping their clients with coping or overcoming their traumas and incidents that happened in the past, and all these were recorded as it was legally required by the Finnish authorities.

The information hacked includes one's name, address, personal identification number, reasons of contacting Vastaamo, goals of the treatments for both client and the authorities.[60] All these information can be used against the victims of this data breach or to hurt their public status or personally attack them as this information that Vastaamo stored is from the most sensitive end of all the information that can be obtained of someone.[61]

Many of the people who have used Vastaamo's therapeutic or medical services in the past, and are at risk that their own personal information have been hacked and possibly had their personal information leaked to the public, have requested their data to be deleted, but their requests have been denied by Vastaamo, based solely on the fact that there's a Finnish regulation from Degree of Ministry of Social Affairs and Health on patient records 298/2009, this regulation actually forces all of the companies working with any kind of medical patients to keep the data saved[62] because the collected data might be needed in the future.

---

59 Sosiaali- ja terveysministeriön asetus potilasasiakirjoista 298/2009
Available online: https://finlex.fi/fi/laki/alkup/2009/20090298
Last accessed 10.2.2022

60 Vastaamo: Tietomurtoja saattoi olla kaksi..-- Helsingin Sanomat, 2020
https://www.hs.fi/kotimaa/art-2000006698960.html
Last accessed 10.2.2022

61 Vastaamo: Tietomurtoja saattoi olla kaksi..-- Helsingin Sanomat, 2020
https://www.hs.fi/kotimaa/art-2000006698960.html
Last accessed 10.2.2022

62 Sosiaali- ja terveysministeriön asetus potilasasiakirjoista 298/2009
Available online: https://finlex.fi/fi/laki/alkup/2009/20090298
Last accessed 10.2.2022

These companies affected by the are not allowed remove any of their existing personal data of their clients without a specific permission from the Finnish authorities to do so[63], as this information may be used by the national authorities. This information may also be used in the court if these people commit a crime or become the victims of one, or if this information can also be requested by other medical institutions, such as public hospitals or health-care centers, which are also located in Finland.

Forced information saving by the government of a certain country can be seen as an issue as it is in contradiction with the GDPR, as the company or organization is forced to keep the saved data even if they are requested by an individual to remove the information, and this has to be done for the reasons stated above, even though the data is forced to be kept, as was the case with Vastaamo[64], they are still responsible for the data and how it is being used, or if a breach of data happens, such as the one mentioned above.

The case above does not seem fair, as they do have control over the saved and processed data but an outer entity, which is above them, is forcing them to keep it instead of deleting it ,[65] even if it was in their own interest to remove it to avoid other responsibilities. Such responsibilities include, for example a possible data breach by unknown entity, which manages to steal all saved personal data, and afterwards shares the stolen personal data with random third parties, as was the case with Vastaamo's data breach.

These two are highly contradicting each other, as GDPR clearly states that the companies or organizations must remove any data relating to data subject if the subject so wishes, but at the same time the national legislation for public interest requires this data to be kept. It comes down to Article 89 of GDPR that can be used by these companies to make the Right to be forgotten unusable at the situation where it is really necessary for public interest to have certain information available and not removed.

63 Sosiaali- ja terveysministeriön asetus potilasasiakirjoista 298/2009
Available online: https://finlex.fi/fi/laki/alkup/2009/20090298
Last accessed 10.2.2022

64 Vastaamo: Tietomurtoja saattoi olla kaksi..-- Helsingin Sanomat, 2020
https://www.hs.fi/kotimaa/art-2000006698960.html
Last accessed 10.2.2022

65 Sosiaali- ja terveysministeriön asetus potilasasiakirjoista 298/2009
Available online: https://finlex.fi/fi/laki/alkup/2009/20090298
Last accessed 10.2.2022

The risks of data collecting and saving are highly visible from the case of Vastaamo, as some of the people who had their personal therapy session information notes and prescriptions stolen by the hackers were contacted and asked for money as a blackmail in order to not have their own information leaked to the public.

Everyone affected by this horrible data breach knows very well that it does not help them at all to go to the police as the hacker was unknown and the information was leaked to the dark web, TOR network, and this actually happened multiple times, everytime through highly secured connections, that even the police can't track.[66]

People who were victims of this data breach had variation of answers, but one was over others: The information is stolen, and there was no certainty that even if the hackers would receive the money they wanted that they would not release the information anywhere, as they were, like stated before, unknown to everyone. The information that is now leaked all over the internet includes Finnish Social Security Number, which can be used maliciously to even take loans on the other persons name without the real own of that Social Security Number knowing.[67]

The responsibility for the hacking is being pushed around by Vastaamo, its old owners, Finnish officials and the victims of the hacking. Everyone has their own opinion on who did wrong, but the bigger issue here is that the information of over 30,000 people is scattered all around the internet, even if it is only on the dark web platform.

The General Data Protection Regulation covers the safeguards and derogations in its Article 89, and it includes safeguards and derogations related to the process for the archiving purposes in the public interest, scientific or historical research or statistical purposes under which the erasure of data is not

66 Ehkä jopa 32 000 Vastaamon potilaan tiedot ilmestyivät viime yönä Tor-verkkoon – poliisi: "Emme tiedä, monenko käsissä tietokanta on", Yle Uutiset, January 2021
https://yle.fi/uutiset/3-11757676
Last accessed 10.2.2022

67 Vastaamo-tapauksesta tehty sata uutta rikosilmoitusta – tietomurto tuli julkisuuteen 4 kuukautta sitten, eikä Sofia, 25, vieläkään tiedä, mitä hänestä netissä kerrotaan, Yle Uutiset, February 2021
https://yle.fi/uutiset/3-11790633
Last accessed 10.2.2022

necessary.[68]

Processing that is done to archive the data over certain public interest, scientific or historical research or statistical purposes, is always subjected to certain safeguards. Those safeguards aim to make sure of that technical and necessarsy organisational measurements are in place in order to secure the compliance to the minimisation of data principle, which means tha the data necessary is only kept. These technical ways can include pseudonymisation given that the purposes of the data can still be fulfilled, and if those purposes may be reached by further processing which does no longer allow the identification of data subjects, those purposes should be done in that way, if the identification of the subjects is not necessary.[69]

If the personal data is processed for scientific or historical research or statistical purposes, EU or its Member State laws might have limitations to the rights referred to in other articles of the GDPR. If for the achievement of specific purposes, or if such derogations are actually needed for the accomplishment of those purposes, or if personally identifiable information that is processed for archiving purposes in the public interest, EU or Member State laws may provide certain limitations from the rights referred to in other articles of the GDPR, as such rights might make it impossible to reach for the specific purposes, and only if these limitations are really necessary.[70]

Article 89 includes many limitations on when certain data has to be kept saved at the database, and thus, cannot be deleted from the the data base. These limitations include public interest, historical, statistical and scientific research purposes,[71] which already limit the information related to

68 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 freemovement of such data, and repealing Directive 95/46/EC. General Data Protection Regulation. Article 89. Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, the technicalities of Art 89.

69 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 freemovement of such data, and repealing Directive 95/46/EC. General Data Protection Regulation., Article 89. Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, on the technicalities of Art 89.

70 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 freemovement of such data, and repealing Directive 95/46/EC. General Data Protection Regulation., Article 89. Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

71 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 freemovement of such data, and repealing Directive 95/46/EC. General Data Protection Regulation., Article 89. Safeguards and derogations

celebrities, historical figures, such as leaders of countries or people who have done something important to be excluded from the possiblity to have their information totally removed, but can still request it to be removed to some extend.

As an example if one happens to be an ex-president of the USA or Russia, it does not mean that if they did something stupid they could not have that information removed, for example if the ex-president ordered few hundred hamburgers for themself or punched their teacher in middle school, that is the kind of information one still could get removed under the Article 17, but for example if they ordered a missile strike on the capital of another country, that's something of public interest and with historical value, and should not be removed from the so called history books.[72]

Article 89 also requires data minimization, meaning that minimal amount of data should be kept saved in order to fullfil the requirements of GDPR while still providing the information necessary to operate. The companies and organizations may use data pseudonymisation, meaning that the data is processed in such manner that it is nearly impossible to connect the data to a single person without additional information being available,[73] and it is one way to minimization of data, as it is nearly impossible with just one record of pseudonymisated data to single out a certain person, instead one would need multiple pseudonymisated records combined to do that.

A way to make sure that the information is no longer under Article 17, or even under the GDPR is anonymisation of the data,[74] which refers to the processing of all personal data in such way that ensures that it is not possible to identify anybody from that saved data.

As an example, this data could even be aggregated to common level or changed into more specific

relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

72 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 freemovement of such data, and repealing Directive 95/46/EC. General Data Protection Regulation., Article 89. Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, more on limitations of the Art 89.

73 Tietosuojavaltuutetun toimisto, Pseudonymised and anonymised data, pseudonymisation https://tietosuoja.fi/en/pseudonymised-and-anonymised-data Last accessed 5.2.2022

74 Tietosuojavaltuutetun toimisto, Pseudonymised and anonymised data, anonymisation https://tietosuoja.fi/en/pseudonymised-and-anonymised-data Last accessed 5.2.2022

statistics so that none could really be identified from the data. This preventation of the possibility of identificating a person from the data must be truly permanent, meaning that it is impossible for the controller or any other party to change the data back into a form where people could be identified from it with all the info posssesed.[75]

This anonymisation of the data has to take into account all the reasonable methods for converting the data to an identifiable form. It must take into account multiple factors, such as the time needed to identify the data subjects, the costs of identification process,[76] and also the available technologies has to be taken into the consideration in the evaluation of the possibility of person's identification.

The controller of the data has to also be prepared for the fact that as the time goes on and the technology advances to new heights, these all can weaken the anonymisation of their saved data. However, the companies do not have to take into account hundreds of years into the future, but instead just the near future, possibly the period of time they have planned to hold on to the information that they do possess.[77]

These safeguard mechanisms mentioned above, anonymisation and pseudonymisation, have to be set out in a way that they ensure respect towards the minimisation of data.[78] These safeguards can be partly or fully ignored in case of public interest, which is probably the most used excuse against GDPR requests by individuals, as almost anything can be made interesting for the public.

Member states, and their supervisory authorities, have the possibility under Article 89 to derogate the original wording in their own legislation if that derogation has a legislative purpose, for

75 Tietosuojavaltuutetun toimisto, Pseudonymised and anonymised data, anonymisation https://tietosuoja.fi/en/pseudonymised-and-anonymised-data Last accessed 5.2.2022

76 Tietosuojavaltuutetun toimisto, Pseudonymised and anonymised data, anonymisation https://tietosuoja.fi/en/pseudonymised-and-anonymised-data Last accessed 5.2.2022

77 Tietosuojavaltuutetun toimisto, Pseudonymised and anonymised data, anonymisation https://tietosuoja.fi/en/pseudonymised-and-anonymised-data Last accessed 5.2.2022

78 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 freemovement of such data, and repealing Directive 95/46/EC. General Data Protection Regulation., Article 89. Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

example, companies working on medical area have to keep their records even if reguested to delete those by the person whose information it is.[79] This possibility for the Member states really does put Vastaamo, and similar companies, in a rough spot, as they have to decide, do they want to go against the National legislation or possibly infringe against the Europen Union legislation.

Simply thinking in a similar case, the company, if looking after their own interests, should go against the National legislation on the Finnish patient records and how they have to be handled[80], as the monetary punishment from breaking it is way lower than it is if they do infringe against the GDPR, which would mean they are going to be sanctioned under the GDPR[81]. However, if a company does break the National law, they are very likely to be revoked of any licenses they have received. This conflict of interest in the two separate legislations causes massive issues for the companies and organizations affected by both of them, as they are forced to balance between these.

79 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 freemovement of such data, and repealing Directive 95/46/EC. General Data Protection Regulation., Article 89. Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

80 Sosiaali- ja terveysministeriön asetus potilasasiakirjoista 298/2009
Available online: https://finlex.fi/fi/laki/alkup/2009/20090298
Last accessed 10.2.2022

81 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 freemovement of such data, and repealing Directive 95/46/EC. General Data Protection Regulation.

1.2 Right to be Forgotten in the US

The fact that United States of America (hereinafter the US) does not really have the right to be forgotten as such does make the research of this chosen topic interesting, however, they do have pieces of legislation that allows individuals to have more privacy. Right to be forgotten can be seen to be a part of those, as some people have tried to enforce legislation similar to the right to be forgotten.

For example, as early as 1931 right to be forgotten was playing a role in the case *Melvin v. Reid* [82], in which Gabrielle Darley, a former prostitute, who had been accused of killing her pimp, but also had been acquitted of the murder, had left that life behind and already had tried to rehabilitate herself back into the society after marrying Bernard Melvin.

Even changing her own last name to Melvin to avoid her past and to try live her life free of the shame that life she had before had brought upon her and her name.[83] And she had at all times lived an honorable, exemplary and righteous way of life. So righteous that she had gained herself a position in a respectable society and had multiple real friends who had not been told of the incidents that took place in her past.

However, during July 1925, the defendants, with no knowledge, permission, nor consent from Gabrielle Melvin, the defendants created, filmed, produced and then released a film titled as "The Red Kimono" and demonstrated the film in the states California, Arizona and many states other aswell.[84]

It had also been clear from the film that it was made to be based on a real story, a story on the past

82 Melvin V. Reid case review, Feb 28, 1931
https://casetext.com/case/melvin-v-reid
Last accessed 10.2.2022
83 Melvin V. Reid case review, Feb 28, 1931
https://casetext.com/case/melvin-v-reid
Last accessed 10.2.2022
84 Melvin V. Reid case review, Feb 28, 1931
https://casetext.com/case/melvin-v-reid
Last accessed 10.2.2022

of Gabrielle Melvin. The fact Darley, which was her maiden last name, was used in the film as the female murderer's name, this was linking Melvin's past together with the film and the story that the defendants wanted to tell with their film.[85]

The whole case, which was originally about monetary compensation, was finally won by Gabrielle Melvin as it was seen by the court that the movie ”The Red Kimono” in which the respondents of the case had used her maiden name, was indeed an invasion to her private life.

As there was no previous cases to justify the judgment in the US the Court of California had to make the decision on the case based on the existing legislation and its provisions, such as the right to pursue and to obtain safety and happiness[86], and as this movie was indeed violation of this right. This precedent case was decided by the court to establish further legislation.[87]

Another important case in the privacy area in the US is from as early as 1940, it is *Sidis v. F-R Publishing*[88] in which a former child prodigy, William James Sidis, sued New York Times for publishing information about his past.

William James Sidis was a quite known child prodigy in the 1910. The name and capabilities of Sidis were not unknown to newspaper readers of the current era of time. For example, at the age of only 11, he lectured to a group of well respected mathematicians over the subject of Four-Dimensional Bodies. Then afterwards when he turned 16, he already graduated from the respected Harvard College, which gave him massive amount of attention.[89]

85 Melvin V. Reid case review, Feb 28, 1931
https://casetext.com/case/melvin-v-reid
Last accessed 10.2.2022
86 Melvin V. Reid case review, Feb 28, 1931
https://casetext.com/case/melvin-v-reid
Last accessed 10.2.2022
87 Precendent, Legal Information Institute, Last updated May 2020
https://www.law.cornell.edu/wex/precedent
Last accessed 5.2.2022
88 Sidis v. F-R PUB. Corporation
https://law.justia.com/cases/federal/appellate-courts/F2/113/806/1509377/
Last accessed 10.2.2022
89 Sidis v. F-R PUB. Corporation
https://law.justia.com/cases/federal/appellate-courts/F2/113/806/1509377/
Last accessed 10.2.2022

After his graduation, Sidis' name had only appeared in the news papers only rarely, and he had tried to live as modestly as he possibly could. He had actually succeeded in his attempts to hide from the public eye, but this was only until these few articles he objected to had appeared in The New Yorker, which revealed his background as a child prodigy. Sidis was indeed once a public figure, but that was back in 1910 as he was a child prodigy, his talents raised both admiration and curiosity. People were expecting great things from him. However, at the time of the publishing of the news articles in 1937, he was working merely as an insignificant clerk, by his own choice, at a place where his mathematical talents were really not giving any real advantage at all.[90]

This case was lost by Sidis as this information was not seen harmful to the plaintiff, even though it was seen as a invasion of privacy. As it is known the US is a country where public interest of the public bodies can be seen to rule pretty much over everything and the freedom of press, in such private life matters of natural persons, is probably the strongest in the world.

In the US anything can be published as long as it has even bit of truth in the article, this makes US an interesting counterpart to EU as they seem to be quite similar when it comes to legislation, but deep inside they are really different from each other in the many ways, such as how the courts rule and how the legislation is drafted.

The first amendment of the US constitution is an important factor as it can indeed be used to make right to be forgotten void when it comes down to media in the US, at least to some extend as shown by the case *Sidis v. F-R Publishing*.[91]

In the US there is not just one massive set of rules, like the EU now has GDPR, that governs the whole area of privacy but instead there are multiple different federal and state laws that are made to protect the privacy of all US citizens, at least that is according to the International Comparative

90 Sidis v. F-R PUB. Corporation
https://law.justia.com/cases/federal/appellate-courts/F2/113/806/1509377/
Last accessed 10.2.2022

91 Sidis v. F-R PUB. Corporation
https://law.justia.com/cases/federal/appellate-courts/F2/113/806/1509377/
Last accessed 10.2.2022

Legal Guides.[92] There is no national level legislation on this area in the US, but the principle of these federal and state laws is the same as EU had before GDPR, where each state can implent and create their own privacy laws, meaning that the total harmonization that the EU now has is missing almost totally.

Lack of real harmonization of the privacy laws actually means that if one state protects people in one way and a company complies with those sets of legislation, the same might not be enough in another state, as some states are more strict than others when it comes to personal privacy of its citizens.

The Federal Trade Commission (herein after the FTC)[93], which is an US government agency promoting and educating people about consumer protection, and enforcing laws to protect consumers from unfair and deceptive business models and practices.[94] The FTC has issued some guidelines regarding on how the data subjects and their information should be handled. These guideline recommendations include the principle transparency, recommending that the privacy notices should be as clear, short and standardized as possible.[95]

Even if there is no legal basis requirements for this processing of data in the US legislation, the FTC can still recommend that companies should do things relating the data subjects in certain way, such as tell these data subjects of the possibility of data collection, as well as about the usage and sharing customs that have been used.[96]

FTC does also recommend that the data collection should be consistent with the context, and that

92 ICLG: Data Protection Laws and Regulations 2020
https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa
Last accessed 10.2.2022
93 United States of America's Federal Trade Commission
https://www.ftc.gov/
Last accessed 12.2.2022
94 United States of America's Federal Trade Commission
https://www.ftc.gov/about-ftc
Last accessed 12.2.2022
95 ICLG: Data Protection Laws and Regulations 2020
https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa
Last accessed 10.2.2022
96 United States of America's Federal Trade Commission's Rules and Recommendations
https://www.ftc.gov/enforcement/rules/rules-and-guides
Last accessed 12.2.2022

data minimization should be in place when certain personal information is being collected from data subjects.[97]

Some of states of the US actually do want to protect the privacy of people and other states on the other hand are more on the side of public information for their own reasons, for example these reasons include statements such as it's used in preventation of crimes or tracking down people suspected of crimes and some for the reason that there just is too much data generated already and is being generated all the time, so it is just kind of a losing game for any company or organization to try to monitor it all.[98]

California has been one of the strictest states when it is matter of the protection over the privacy of people. On June 2018 the Senate and Congress in California unanimously voted for passing California Consumer Privacy Act of 2018, which will make it the strictest state in this area, giving consumers more rights over their own information.[99]

However, as disappointing as it sounds in the comparison to the GDPR, this California's Consumer Privacy Act of 2018 only does apply to the area of state of California,[100] as it was stated earlier each US state has their own set of state laws that apply only on their own territory.

Even if this might be the first step on the road towards other states following California in passing similar laws, most likely those laws will still vary at least on the way those will be written or implemented into the judicial system due to the lack of national harmonization in the US.[101]

---

97 ICLG: Data Protection Laws and Regulations 2020
https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa
Last accessed 10.2.2022

98 Cameron F. Kerry , Why protecting privacy is a losing game today—and how to change the game. July 2018
https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/
Last accessed 10.2.2022

99 California Consumer Privacy Act of 2018
https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375
Last accessed 5.2.2022

100 California Consumer Privacy Act of 2018
https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375
Last accessed 5.2.2022

101 ICLG: Data Protection Laws and Regulations 2020
https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa
Last accessed 10.2.2022

The lack of harmonization in the US makes it really tough for ordinary people to really know or understand whether something is allowed in one state if it was allowed in another state, or the opposite way around, if something was illegal on another state if it also is illegal in the other states aswell.

However, this lack of harmonization also opens possibilities for people to take advantage of the states which are not as strict as California for example, and setting headquarters of their company there to avoid certain judicial restrictions that are in place for the companies operating inside the more strict states.[102]

The Electronic Communications Privacy Act of California does prevent the law enforcements, or the investigative entities from making a company forced to give them their electronic form of data or communications without any warrant obtained from the court.[103] This includes cloud data, the meta data, emails sent and received, aswell as text messages, location data and seearches done by devices. Some of the states do also have certain laws that protect some of these forms of collected data, However, California is as of now the only state that actually protects these all.

The contrast in the US is massive when it comes to the privacy laws, While some states do not have any laws to protect a journalist from having to expose the sources they have used, Wyoming as a state, does even not even have any court precedent for it. In addition, in the state of Wyoming the companies or organizations are actually not even required by law to delete their collected personal data of their customers after a certain period of time.[104] Even more worrying is that in the state of Wyoming the employers are allowed to force their employees to give them their passwords used to their personal social media accounts.

---

102 California Consumer Privacy Act of 2018
https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375
Last accessed 5.2.2022

103 The Electronic Communications Privacy Act of California: Senate Bill No. 178, An act to add Chapter 3.6 (commencing with Section 1546) to Title 12 of Part 2 of the Penal Code, relating to privacy. October 8, 2015
https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201520160SB178
5.2.2022

104 Paul Bischoff. Internet Privacy Laws by State: which US states best protect privacy online?, Comparitech October 23, 2019
https://www.comparitech.com/blog/vpn-privacy/which-us-states-best-protect-online-privacy/
Last accessed 8.2.2022

Even if California has the highest amount of privacy laws in effect, and are ranked as the best state when it comes to the individual privacy, the state of Illinois is actually the only state in the whole US that has successfully passed a law for specifically protecting collected biometric data, which includes for example face scans used for recognition, fingerprints and scans of eye's retina. Companies, organizations and even the governmental bodies must delete their collected personal data after a certain amount of time.[105] Another thing worth mentioning is that in Illinois schools are not allowed to force their teachers or other people working there or people studying there to give them their personal social media account login information.

As the coin always has two sides, it opens door for people to take advantage of the strictness of the Californian legislation, and sueing companies in the Courts of California to get possibility for a better compensation reward awarded by the courts comparison to the one they would get in a state, for example Wyoming,[106] that has next to no legislation on the Privacy area.

The Privacy Act of 1974, which concerns the executive agencies the US government, applies only to US citizens, and to people who have been lawfully admitted for a permanent residence in the US area. It is only applicable to personal information maintained by these agencies, and as most of the privacy laws in the US enforcement of criminal punishments or investigations are excluded from the Privacy Act. The Central Intelligence Agency (hereinafter CIA) and its records are always excluded from any privacy laws in order for the CIA to fully operate and perform its own tasks relating to crime investigation and preventation.[107]

105Paul Bischoff. Internet Privacy Laws by State: which US states best protect privacy online?, Comparitech October 23, 2019
https://www.comparitech.com/blog/vpn-privacy/which-us-states-best-protect-online-privacy/
Last accessed 8.2.2022

106Paul Bischoff. Internet Privacy Laws by State: which US states best protect privacy online?, Comparitech October 23, 2019
https://www.comparitech.com/blog/vpn-privacy/which-us-states-best-protect-online-privacy/
Last accessed 8.2.2022

107US Small Business Administration, Privacy Act of 1974
https://www.sba.gov/about-sba/open-government/privacy-act
Last accessed 15.2.2022

2. Fines and sanctions for non-compliance

Due to the fact that no law will actually work in a long run without it having some sanctions behind it, the GDPR as well as the US laws have sanctions and fines that are imposed on the violators by the EU, or in US case by the states.

The punishment for non-compliance and violations of the laws are given to the companies or organizations meaning that they are monetary punishments and sometimes may also include a block from operating if the violation is truly severe in its nature.

GDPR has set out limits to what the fines can be and what they should be in different cases of non-compliance, meaning that it is quite easy for anyone to see how their company or organization will be punished if they do something that violates the GDPR.[108]

In the GDPR regime, the size of the company and their assets do play a significant role when determining what is the correct amount in Euros, within the boundaries set out by the GDPR. However, the severity of the infringement, does also have an effect on how big the fine and sanctions will be.

Also these fines and sanctions for non-compliacen with the GPDR can be imposed on companies and organizations outside of the area of the EU, as long as they are doing business with EU citizens, or actually anyone residing within the EU borders.[109]

When it comes to the US and their sanctions, or fines, for non-compliance with certain legislation, it is in the hands of the court to determine what is the correct amount of fine or compensation that the company or organization, which has violated the US privacy laws, has to pay.[110] This is why the

108REGULATION (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 freemovement of such data, and repealing Directive 95/46/EC. General Data Protection Regulation.

109REGULATION (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 freemovement of such data, and repealing Directive 95/46/EC. General Data Protection Regulation.

110Judicial Remedies and Penalties for Violating the Privacy Act, The United States Department of Justice,

fines may vary from small to many hundred billions of dollars.

As the possible compensation amounts awarded in the US are way bigger than in the EU, people are more likely to bring a civil suit against a company or an organization if they know they have done something wrong, in order to gain personal advantage of it, meaning they do receive monetary compensation when the company or organization is found guilty, by the court, for violating the US privacy laws.

The difference in the systems are quite big, as EU is harmonized system, where each Member state should have pretty similar fines and sanctions for the violations. At the same time in the US each of the 50 states has their own system, and own methods of determining what the correct fine or sanction should be.

The European GDPR regime and its harmonization closes the door for possible forum shopping, meaning the plaintiff could choose the court in which they could bring the claim forward from the courts that are able to exercise jurisdiction on the matter at hand, and choosing the court that is most likely to provide them with the best outcome.[111] However, in the US this can possible be done as most of the companies do operate on multiple states, not to mention the ones operating world wide.

https://www.justice.gov/jm/eousa-resource-manual-142-judicial-remedies-and-penalties-violating-privacy-act
Last accessed 8.2.2022

111 Legal definition of: Forum Shopping, Merriam-Webster Legal Dictionary
https://www.merriam-webster.com/legal/forum%20shopping
Last accessed 5.2.2022

2.1 GDPR's fines and penalties for non-compliance

Right to erasure does not limit people from speaking about a case or information that might be harmful for one's future or even future employment but it will limit the media and especially social media from being used as a platform to do so as the monetary penalty for non-compliance with the GDPR is hefty for big companies such as Facebook, Instagram or Google, as they are still to some extend responsible what is posted on their services, even if it is private individuals doing it on their own.[112]

Media platforms such as online news papers and television broadcasting services are also liable for anything that they post or broadcast online under the GDPR. So they also must act in accordance with the GDPR even if they are broadcasting from abroad if their service is available for anyone residing in the area of the European Union.[113]

European General Data Protection Regulation lays out the levels of sanctions in its Article 83, that companies and organizations would receive for different kind of infringements against the GDPR. These supervisory authorities have to make sure that the imposition of administrative fines are necessary and hefty enough for infringements. Authorities must also make sure that in each individual case these sanctions effective, proportionate and dissuasive.[114]

These so called administrative fines depend on the circumstances of each case. When authorities decide if a fine is necessary and what a correct amount of the administrative fine in the case should be they have to take into consideration the nature, seriousness and time of the infringement in relation to the purposes of the data processing. Number of data subjects who have been hurt and

112REGULATION (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 freemovement of such data, and repealing Directive 95/46/EC. General Data Protection Regulation.

113REGULATION (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 freemovement of such data, and repealing Directive 95/46/EC. General Data Protection Regulation.

114REGULATION (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 freemovement of such data, and repealing Directive 95/46/EC. General Data Protection Regulation., Article 83: General conditions for imposing administrative fines, how Art 83 works.

what kind of damages has been caused to them.[115]

Supervisory authorities must also take a look whether the infringement was intentional or not, and where the controller or processor had done anything to limit the damages caused to the subjects. The responsibilities of the data controller or processor are also taken into account when looking at the technical and also organisational precautions implemented by these two. The possible previous violations by them and the level of their collaboration with the authorities in order to solve the violations and limit the occuring negative effects of their infringement, and also the types of personal data included in this infringement are closely looked at when deciding the level of the sanctions.[116]

The way in which the infringement became to the knowledge of the authorities, whether the controller or processor notified about it or if they tried to hide it instead. The financial gains, or losses, due to the infringement must also be taken into consideration when sanctions are given in the case. The amount may still not exceed the highest amount allowed by the regulation even if there are multiple infringements.[117]

There are two levels of fines that can be given for the infringements. First one is lower and second one is about double the amount. These two depend highly on the nature, seriousness and time of the infringements as well as other factors mentioned above. Authorities may hand out administrative fines up to ten million Euros, or in the matter of a business, they may give a fine up to two percent of the total worldwide annual turnover of the preceeding financial year, and whichever of these two is higher will be handed out. Authorities may hand out administrative fines up to to 20 million Euros, or in the case of a business, they may give a fine up to four percent of the total worldwide annual turnover of the preceeding financial year, and again, whichever of these two is higher will be

115GDPR-info, Art. 83 GDPR, General conditions for imposing administrative fines, 2018
https://gdpr-info.eu/art-83-gdpr/
Last accessed: 10.2.2022

116REGULATION (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 freemovement of such data, and repealing Directive 95/46/EC. General Data Protection Regulation., Article 83: General conditions for imposing administrative fines, how Art 83 works.

117REGULATION (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 freemovement of such data, and repealing Directive 95/46/EC. General Data Protection Regulation., Article 83: General conditions for imposing administrative fines, how Art 83 works.

given as a fine.[118]

If a company or organisating does not comply with an order given by the authorities the authorities may give administrative fines up to to 20 million Euros, or a hefty fine up to 4% of the total worldwide annual turnover of the preceeding financial year.[119]

Every Member State of the EU may place certain rules on when and how easily administrative fines will be imposed on their public. This can be done without any precedent from the corrective powers of current supervisory authorities. And these authorities must follow appropriate safeguarding mechanisms, such as due process of law and include effective judicial remedies in the actions the take or do under the powers vested in them.[120]

Article 83 does cover these infringements even if the Member State's own legal systems does not have these fines in place, the fines are just initiated by the current authorities in power and then imposed by the national courts, which will ensure that the legal remedies are indeed in place and that these fines are effective and actually necessary. Member States will have to notify the Commission of the sections of the laws which they will be adopting without delay, any other amendments of law that will be affecting them.[121]

As there are two levels of administrative fines possible under the Article 83 of GDPR for the non-compliance with the GDPR. First one being lower and the second level being much higher, and one of them will be imposed on the company which does not follow the GDPR. The level of the fine

118 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 freemovement of such data, and repealing Directive 95/46/EC. General Data Protection Regulation. Article 83: General conditions for imposing administrative fines, how Art 83 works.

119 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 freemovement of such data, and repealing Directive 95/46/EC. General Data Protection Regulation., Article 83: General conditions for imposing administrative fines, how Art 83 works.

120 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 freemovement of such data, and repealing Directive 95/46/EC. General Data Protection Regulation. Article 83: General conditions for imposing administrative fines, how Art 83 works.

121 GDPR-info, Art. 83 GDPR, General conditions for imposing administrative fines, 2018
https://gdpr-info.eu/art-83-gdpr/
Last accessed: 10.2.2022

depends on the infringement's severity.[122]

These minor infringements would result in a hefty fine up to ten million Euros or two percent of the company's worldwide annual revenue from the preceding financial year, and the higher of these two would be applied. These fines are severe for a smaller companies, however a big technological giant such as Apple or Google, might not care if they are handed a fine, but instead just pay it and maybe do something about the issue that caused them to get the huge fine at the first place. [123]

The more severe infringements could in other hand result in a bigger fine up to 20 million Euros or four percent of the company's worldwide annual revenue from the preceding financial year, and again, the higher of these fines will be applied to make sure that even big companies would imply the boundaries set by the GPDR in their actions, as 20 million Euros fine to a multi-billion company would not have as good effect as the percentual fine will.[124]

Due to the fact that the society today is constructed in a way that people do not follow the guidelines, or laws, unless there is a possibility to receive a punishment for breaking that said rule. The bigger the possibility to receive a punishment, as in monitoring and punishing the people makes it more likely that they do indeed follow the laws.

Given the severity of the possible fine or prison sentence also plays a major role in whether people follow the laws, and as the GDPR does not include prison sentences for non-compliance with it, the fines are given a much stronger emphasis in order to make people follow the GDPR as part of the legislation.[125]

---

122 What are the GDPR fines? Two tiers of GDPR fines
https://gdpr.eu/fines/
Last accessed 5.2.2022

123 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 freemovement of such data, and repealing Directive 95/46/EC. General Data Protection Regulation., Article 83

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 freemovement of such data, and repealing Directive 95/46/EC. General Data Protection Regulation.

125 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 freemovement of such data, and repealing Directive 95/46/EC. General Data Protection Regulation.: Article 17. Right to erasure

For example, a simple fine for speeding is not so severe that some people willingly take their chances in driving over the speed limit, but if you compare a few hundred Euros worth of fine for speeding[126] to a person compared to a prison sentence for stealing something or murdering someone[127], and lastly comparing those to at least multiple millions worth of penalty sanction for an organization or a company for each breach of the law[128], it helps to put the amount of the fine to perspective.

Given that every company's main objective is to make money, so they might not want to be willing to give such amount of extra money away, for basically free, if they have the possibility avoid that by simply following the regulations of the GDPR, which on the other hand are not that hard to cooperate with.

Even though the fine is the biggest scare of the penalties that GDPR allows EU's authorites to impose on companies or organizations that violate its regulations, there are other factors that could be considered as penalty for non-compliance. The fact that the people whose personal data has been breached or leaked can make claims for personal compensation from the company or organization, and the amount they will receive depends on the severity of the breach.

For example, one's name being leaked might not be as bad in terms of compesation amount as if their home address and payment information have also been leaked, and this is a possibility for any company that either collect, process or analyze any data regarding any European resident, not just European Union's citizens, as that it is what a data subject includes in the GDPR.[129]

The fines are seen to be a harsh enough punishment by the European Union's deciding organs. On

126Finnish Police's fine procedure and fines
https://www.poliisi.fi/crimes/fine_procedure
Last accesssed 5.2.2022

127Official Statistics of Finland (OSF): Prosecutions, sentences and punishments [e-publication]
http://www.stat.fi/til/syyttr/2019/syyttr_2019_2020-09-24_tie_001_en.html
Last accessed 5.2.2022

128What are the GDPR fines? Two tiers of GDPR fines
https://gdpr.eu/fines/
Last accessed 5.2.2022

129REGULATION (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 freemovement of such data, and repealing Directive 95/46/EC. General Data Protection Regulation.: Article 17. Right to erasure

the other hand a possibility for a prison sentence could be a personal scare, as it would amount to both loss of income and loss of freedom, instead of monetary loss as set out in the GDPR at the very moment[130]. If there was a possiblity for the most severe cases to result in a prison sentence, even the companies considered untouchable by the laws, such as Facebook, Amazon or Google, would be even more likely to operate within the exact lines and not trying to bend them into their own favour.

As these companies mentioned above, do have billions of Euros, or Dollars, to spend, but we all only get a lifetime to spend, and if the owner of the company or organization would get, for example a five to ten years imprisonment for the data breaches your company has done under your control, you'd be way more cooperative and willing to follow the guidelines and also people would be more likely to do their best to make sure that their employees were actually following the regulations to their best abilities to do so, instead of just paying of a fine.

However, big companies aren't run by just one person, they have a team or multiple teams running different parts of the company, for example one part might responsible for advertisement, one takes care of the budget and one handles the data collected or processed.

Even if the owner of the company would be convicted for something that he might have hired people to work with, would that be seen as fair actions against them, or should the imprisonment include only the people responsible of the breach or also their leaders, if they were aware of such breaches being done. So all in all the fines alone should be good enough to make companies to operate within the area set by the GDPR.

People usually demand that also the people that caused the harm while working for the company to should be held responsible for the harm the company has done, whether it is to the nature or to someone else, but as the GDPR does not include prison sentences, as would be possibility for causing some natural disaster by leaking oil or some other dangerous substance to the seas, should there also be fines targeted to the individuals or is the fines that the company receive a punishment enough, as it is loss of profit.[131]

130REGULATION (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 freemovement of such data, and repealing Directive 95/46/EC. General Data Protection Regulation.: Article 17. Right to erasure

131A Mitchell Polinsky and Steven Shavell - International Review of Law and Economics: Should Employees Be

Too hefty fines and too small area to operate in could also have a negative effect on the services and products provided into the EU, as companies would not want to risk having face huge problems with law for some breach that might even be out of their hands, this could, and somewhat already did before GDPR even came to force, result in different methods such as geo-blocking, meaning that certain areas out of the reach of use of certain services on the internet.

This was done to limit the possibility of GDPR's applicability to limit the data the companies process or store,[132] as working one's way around the geo-block can be considered illegal as that includes use of external computer programs, thus making the company possibly breaking some regulations set out by the GDPR non neglient as they were no longer providing services to the European Union or its residents.

The possibility to access the services from the EU already create the reguirement to follow the GDPR for the company, however, if this possibility to access the services from EU is restricted the company or organization does not have to comply with the GDPR, as they are not actually providing services or doing business with the residents of the EU.[133]

Fines and penatlies that the European data protection authorities have so far imposed range from few thousand Euros to 50 million Euros. This shows that the European authorities working with the GDPR infringements are truly imposing the fines and penalties. These fines take into account the severity of the infringement as well as the size of the company or organization in charge of the failure to fullfil the GDPRs requirements.

For example of a smaller fine imposed by the GDPR authorities on companies failing to follow the

Subject to Fines and Imprisonment Given the Existence of Corporate Liability? https://www.sciencedirect.com/science/article/abs/pii/0144818893900354?via%3Dihub Last accessed 10.2.2022

132 Alex Hern and Jim Waterson – Sites block users, shut down activities and flood inboxes as GDPR rules loom, The Guardian, May 2018 https://www.theguardian.com/technology/2018/may/24/sites-block-eu-users-before-gdpr-takes-effect Last accessed 10.2.2022

133 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 freemovement of such data, and repealing Directive 95/46/EC. General Data Protection Regulation.

GDPR, the Finnish company, Posti Group, which is responsible for most of the mail distribution in Finland was handed a 100,000 Euros fine for infringement of GDPR.[134] These infringements were made during the handling of data, as the sharing of the data to third parties, for example telemarketing companies, by Posti Group.[135]

An example of a bigger fine, and actually the biggest fine so far, imposed for failing to fullfil the requirements of the GDPR was handed to Google LLC. They received a huge fine of fifty million Euros for multiple infringements in early 2019, these infringements did also include the Article 17 of the GDPR being violated.[136]

The fine was imposed by National Commission on Informatics and Liberty, also known as the CNIL, on Google for having issues of transparency, delivering unaccurate information on the use of the personal data collected and finally for missing certain consent requirements regarding their personalization of targeted ads.[137]

Google had done almost everything they needed to do, and they did it almost correctly, but the information on what was collected and how it was used just was too vague on its wording, meaning that the person who had their personal data collected by Google might not have fully understood why and how the data was being gathered, stored and used by Google. Also the transparency of the information was not transparent enough for the European data protection authorities.[138]

134GDPR Enforcement tracker for fines imposed by the European data protection authorities
https://www.enforcementtracker.com/
Last accessed 8.2.2022

135Tietosuojavaltuuten toimisto, Postin rikkeet Euroopen tietosuojalaissa. 18th May 2020
https://tietosuoja.fi/documents/6927448/22406974/Henkil%C3%B6tietojen+k%C3%A4sittelyn+l%C3%A4pin%C3%A4kyvyys+ja+rekister%C3%B6idylle+toimitettavat+tiedot.pdf/b869b7ba-1a05-572e-d97a-9c8a56998fc1/Henkil%C3%B6tietojen+k%C3%A4sittelyn+l%C3%A4pin%C3%A4kyvyys+ja+rekister%C3%B6idylle+toimitettavat+tiedot.pdf
Last accessed 8.2.2022

136GDPR Enforcement tracker for fines imposed by the European data protection authorities
https://www.enforcementtracker.com/
Last accessed 8.2.2022

137The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC, 21st January 2019,
https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc
Last accessed 5.2.2022

138The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC, 21st January 2019,
https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc
Last accessed 5.2.2022

Google even appealed on the decision made by the CNIL to avoid having to change their policies and the fine, but the French Highest Administrative Court upheld the CNIL decision of the 50 million Euros fine for the GDPR violations.[139]

This is a major decision showing that even the biggest companies do get punished for GDPR related violations, even though the monetary sanction isn't so massive for a multi-billion internet giant, as Google is.

These two above mentioned cases are from the opposite ends of the spectrum of the GDPR related fines and sanctions, and as it can be seen Google as one of the biggest, if not the biggest, company in the whole world had to pay way bigger fines than a smaller company that's basically only operating in a single country.

The fines were seen as too big in the beginning but now that the GDPR has been enforced for few years, it can be seen that all these fines are reasonable and should not make companies go bankrupt for a single GDPR related mistake, as one mistake may not even lead to a fine, as long as the issue is corrected as soon as it is brought to the attention of the company.[140]

The difference between a simple human mistake and someone willingly doing something wrong is truly narrow, and it is why the supervisory authorities of each Member state[141] have to be precise when they do weight the infringement towards the fine, and what could have been done differently. Of course some cases are clear and the companies are punished according to what they deserve for their GDPR related violations.

139GDPR: the Council of State rejects the appeal against the sanction of 50 million euros imposed on Google by the CNIL, June 2020
https://www.conseil-etat.fr/actualites/actualites/rgpd-le-conseil-d-etat-rejette-le-recours-dirige-contre-la-sanction-de-50-millions-d-euros-infligee-a-google-par-la-cnil
Last accessed 10.2.2022

140REGULATION (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 freemovement of such data, and repealing Directive 95/46/EC. General Data Protection Regulation.

141REGULATION (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 freemovement of such data, and repealing Directive 95/46/EC. General Data Protection Regulation.

Companies also do have a month to respond to any request they receive, and the period can be requested to have extension of two months if the request is complex or includes multiple requests. Another thing to mention is that the companies have to react to these requests free of charge, meaning even though they are paying someone to do this, the one requesting, for example their information to be removed, can do it free.[142]

142Data protection under GDPR, European Union – Your Europe, 2021 https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_en.htm Last accessed 10.2.2022

2.2 US fines and penalties for the non-compliance with Privacy laws

In the United States of America, due to the country being a federation, the fines and penalties for anything related to breaking the law or getting a fine varies heavily depending on the state where the law has been broken at, and the severity of the breach at hand. In some cases things that are illegal on another state are allowed in another one.

This can be taken advantage of by companies and organizations by simply setting their main operations to the states where for example selling ones customers' personal information is not limited by law.[143]

Privacy was seen as secondary right after the terrorist attacks of September 2001 on the US, as tracking down the criminals and the terrorist became more and more important to the deciding people of the US.[144] This was due to the common feeling that their safety was compromised by the unwanted people staying in their territory, or still trying to get into the US.

USA has always been seen around the world as a police state, where police has the authority to do almost anything they want and it is always under the law, or sometimes even be above the laws that they should operate within, as long as they can justify it with the need or good for the most of the people, such allows them almost illegal searching of premises or detaining people in order to create peace to most of the people.

Privacy rights are something that should not have been waived, but that sadly was the case in the US, and the public was seen as a better approach as it allowed the government to act easier on tracking down the terrorists that were residing inside the US. Even though the cost if this was lack

143 Anita L. Allen, Unpopular Privacy – What Must We Hide? Part I
Oxford University Press, 2011
Ebook available on https://play.google.com/store/books/details?id=91NpAgAAQBAJ&rdid=book-91NpAgAAQBAJ&rdot=1&source=gbs_vpt_read&pcampaignid=books_booksearch_viewport
Last accessed 10.2.2022

144 Anita L. Allen, Unpopular Privacy – What Must We Hide? Part II
Oxford University Press, 2011
Ebook available on https://play.google.com/store/books/details?id=91NpAgAAQBAJ&rdid=book-91NpAgAAQBAJ&rdot=1&source=gbs_vpt_read&pcampaignid=books_booksearch_viewport
Last accessed 10.2.2022

of privacy for ordinary people in their everyday life it was seen as the best solution at that time to the most of the people.[145]

Taking California as an example as they have been the most pro-active when it comes to the privacy of the normal people. So pro-active that already in 2003 a law called ”Shine the Light” was passed which actually did somewhat the same for individuals and their privacy, as the GDPR now strengthens in the EU.[146]

When it comes to sanctions in the US, they are not always only monetary, but might also include seizure of property or assets. The Attorney General of the US may also institute civil actions to order any governmental entities to start complying with all the conditions and requirements of the current legislation in force.[147]

”Shine the Light” empowered any Californian individual to be able to either optain information from any company or organization they are dealing with on how their personal information is being shared for direct marketing.[148]

However, companies with under twenty employees are excluded from the Shine the Light laws requirements, together with the federal financial institutions that also have been exempt from the requirements.[149]

---

145 Anita L. Allen, Unpopular Privacy – What Must We Hide? Part II
Oxford University Press, 2011
Ebook available on https://play.google.com/store/books/details?id=91NpAgAAQBAJ&rdid=book-91NpAgAAQBAJ&rdot=1&source=gbs_vpt_read&pcampaignid=books_booksearch_viewport
Last accessed 10.2.2022

146 California Legislative Information, S.B. 27, Shine the Light law of 2003
https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=1798.83.&lawCode=CIV
Last accessed 5.2.2022

147 The Electronic Communications Privacy Act of California: Senate Bill No. 178, An act to add Chapter 3.6 (commencing with Section 1546) to Title 12 of Part 2 of the Penal Code, relating to privacy. October 8, 2015

148 California Legislative Information, S.B. 27, Shine the Light law of 2003
https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=1798.83.&lawCode=CIV
Last accessed 5.2.2022

149 California Legislative Information, S.B. 27, Shine the Light law of 2003
https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=1798.83.&lawCode=CIV
Last accessed 5.2.2022

Given that the GDPR actually does force companies and organizations within or outside the EU to comply with it in order to avoid the fines and sanctions. This is very contradictiory to the way the same works in the US.

Most of the US privacy legislation does not require even US or foreign companies or organizations, or their officers, employees, or agents to take any steps for actually providing information, records, facilities, or any other forms of assist in agreement with the conditions of warrants, court orders, statutory authorizations, emergency certifications, or wiretapping orders issued[150].

This all has to be done by the police or authorities investigating the case at hand. Of course the companies or organizations or anyone working there are allowed to help the authorities, and are most likely to be rewarded with something for their assistance.

This reward could include things such as smaller fines or other less harsh sanctions. Also it may be even possible to enter into negotiations with the plaintiff(s) if the companies or organizations cooperate with the investigating bodies directly from the beginning.[151] They usually do assist in order to avoid a possibly harsh court decision against them.

US does not have a separate authorities monitoring and investigating on the companies or the organizations on their own, but instead individuals have to bring a civil claim to a federal court in order to have the issue investigated by the authorities and be awarded with compensation for the damages the willful or intentional non-compliance by the companies or organizations has caused the plaintiff.[152]

---

150 The Electronic Communications Privacy Act of California: Senate Bill No. 178, An act to add Chapter 3.6 (commencing with Section 1546) to Title 12 of Part 2 of the Penal Code, relating to privacy, 1546.4 (d). October 8, 2015
https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201520160SB178
Last accessed 5.2.2022

151 Judicial Remedies and Penalties for Violating the Privacy Act, The United States Department of Justice,
https://www.justice.gov/jm/eousa-resource-manual-142-judicial-remedies-and-penalties-violating-privacy-act
Last accessed 8.2.2022

152 Judicial Remedies and Penalties for Violating the Privacy Act, The United States Department of Justice,
https://www.justice.gov/jm/eousa-resource-manual-142-judicial-remedies-and-penalties-violating-privacy-act
Last accessed 8.2.2022

These compensations for damages in the US can reach billions of dollars, which is why people are more willing to negotiate behind closed doors to settle the compensation amount to be a reasonable amount.

As there are no real set out amounts of fines or compensation on a federal level, each court can decide what they see just as compensation compared with the damages that the company or organization has actually caused to the plaintiff(s)[153].

The above is the reason why some of the biggest fines and sanctions in the US have reach multiple hundred billion dollars, and these huge fines are quite common in the US,[154] where as in EU biggest fines have reached up to multiple hundred million Euros, such as Googles 50 million Euros fine for non-compliance with the GDPR.

153Judicial Remedies and Penalties for Violating the Privacy Act, The United States Department of Justice, https://www.justice.gov/jm/eousa-resource-manual-142-judicial-remedies-and-penalties-violating-privacy-act Last accessed 8.2.2022

154 5 of the Most Expensive Court Cases in US History, Connorreporting, 2021 https://connorreporting.com/5-expensive-court-cases-us-history/ Last accessed 10.2.2022

3. Monitoring of non-compliance

The EU and the US both have their own methods regarding the monitoring of the non-compliance of their data protection legislations.

The GDPR can be seen as a world wide legislation, as it regulates every company or organization doing business or providing services to the residents of the EU, even though it is only implemented to the EU's own legislations and to the EU Member states legislation, which should be in harmony with the GDPR.[155]

The level of harmonization of the privacy laws and rights in the EU is way higher than in the US, as in the US every state has their own privacy laws and rights. The US, with little federal level of legislation on the matter, has allowed their states to implement their own methods and authorities for monitoring non-compliance with the laws.[156] These methods, and laws, vary between the states and what they do prioritize more, the privacy of individuals or the public's actual interest to the information.

155REGULATION (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 freemovement of such data, and repealing Directive 95/46/EC. General Data Protection Regulation.

156ICLG: Data Protection Laws and Regulations 2020
https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa
Last accessed 10.2.2022

3.1 Monitoring of the non-compliance of the GDPR

The authorities that are mainly responsible for dealing with the monitoring of the compliance of GDPR in the EU are national institutions operating under the specifications laid out in the GDPR Articles 51 to 59 and set out by the EU Member states. However, if a private person notices that their rights under the GDPR may have been breached they can turn to one of these institutions and have this breach investigated and the company or organization responsible for the breach may get fined and penalized.[157]

These authorities must work together with other EU Member States to make sure of that each and every of these authorities are working in harmony under the GDPR. This harmonization includes the fines and penalties aswell as the means usable by the authorities in tracking down non-compliance by companies or organizations in relation to any of the EU citizens.[158]

People can request the GDPR related authorities of the EU member state to have an investigation over a certain company whether a breach of data, leak of personal information or other similar misuse of information has taken place. The authorities will then have an investigation to determine if the company is operating in compliance with the GDPR or not. They will then issue monetary penalties as in fines under the GDPR regime in addition to or instead of other remedies.[159]

As the European data protection authorites get requests from just one person to investigate these possible infringements they may search for additional infringements while they are investigating for just one or two complaints or request by individuals, and if any additional infringements are found the company will receive multiple charges for the failure to fullfil the requirements of GDPR as was the issue with the Finnish company Posti Group, where just few complaints lead the data protection

157REGULATION (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 freemovement of such data, and repealing Directive 95/46/EC. General Data Protection Regulation.

158REGULATION (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 freemovement of such data, and repealing Directive 95/46/EC. General Data Protection Regulatio: Chapter VI

159REGULATION (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 freemovement of such data, and repealing Directive 95/46/EC. General Data Protection Regulation.: Article 83

authorities to find multiple violations and causing Posti Group to receive higher fines than what they would have received from a single violation.[160]

The supervisory authorities' powers in the EU have been laid out in the Article 58 of the GDPR. These supervisory authority should have investigative powers, which allow them to order the controllers, the processors, or the controller's or the processor's representatives to give out any information required to fullfil investigative tasks. These powers also allow them to carry out investigations in the form of inspections, or to review certain certifications at question by the GDPR.[161]

These authorities may also notify controllers or processors of a possible violation of GDPR. They may reach out to a controller and a processor and request an access to the personally identifiable data collected, other information needed, obtain access to the premises of them, even the equipment used relating to any data activities, as long as it is in harmony with EU or Member State's procedural laws.[162]

Supervisory authorities' corrective powers allow them to issue warnings or reprimands to anybody, whether controller or processor if those are infringing against the GDPR. Authorities with the corrective powers may also request controllers or processors to actually comply with these requests from data subjects under GDPR. Another thing authorities could do is to force company's processing activities into complying with the GDPR, and give specific timeline to do so, this also includes the need to tell subjects that their data has been possibly breached. Authorities may also impose a permanent or temporary blocking over processing if certain areas of GDPR are not being

160Tietosuojavaltuuten toimisto, Postin rikkeet Euroopan tietosuojalaissa. 18th May 2020 https://tietosuoja.fi/documents/6927448/22406974/Henkil%C3%B6tietojen+k%C3%A4sittelyn+l%C3%A4pin%C3%A4kyvyys+ja+rekister%C3%B6idylle+toimitettavat+tiedot.pdf/b869b7ba-1a05-572e-d97a-9c8a56998fc1/Henkil%C3%B6tietojen+k%C3%A4sittelyn+l%C3%A4pin%C3%A4kyvyys+ja+rekister%C3%B6idylle+toimitettavat+tiedot.pdf
Last accessed 8.2.2022

161REGULATION (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 freemovement of such data, and repealing Directive 95/46/EC. General Data Protection Regulation., Article 58, Powers of the Supervisory authorities, Corrective powers

162REGULATION (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 freemovement of such data, and repealing Directive 95/46/EC. General Data Protection Regulation., Article 58, Powers of the Supervisory authorities. Investigative powers

followed by the controller or processors.[163]

Authorities may also force requests of the correction or erasing of personal data or restrictions of processing of data under Articles 16, 17 and 18 of the GDPR. They may also force a removal of a certification or to force a certain certification body to withdraw a certification that they have previously issued. Supervisory authorities also do have the powers to impose fines under Article 83 of the GDPR, or even suspend data from being shared around even if the receiver would not be inside EU.[164]

Supervisory authorities should also have some authorisation and advisory powers. They have the ability to advise controllers in according to the previous consultation procedures. They may also authorize any processing, if laws of a Member State requires such authorisation.

These supervisors may give their opinion and even approve certain drafts of codes of conduct or authorize certification body, if such is necessary, or even hand out certifications and pass criterias for certifications or assume standard clauses for data protection or authorize certain administrative arrangments or pass corporate rules in relation to the GDPR.[165]

The use of the powers granted to these supervisory authories are required to be only used under certian safeguarding mechanisms, these include, for example, effective judicial remedy and due process of law.[166]

163REGULATION (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 freemovement of such data, and repealing Directive 95/46/EC. General Data Protection Regulation., Article 58, Powers of the Supervisory authorities

164REGULATION (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 freemovement of such data, and repealing Directive 95/46/EC. General Data Protection Regulation.

165REGULATION (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 freemovement of such data, and repealing Directive 95/46/EC. General Data Protection Regulation. Article 58, Powers of the Supervisory authorities

166REGULATION (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 freemovement of such data, and repealing Directive 95/46/EC. General Data Protection Regulation., Article 58, Powers of the Supervisory authorities

These authorities must have the capability to bring to the attention of the national courts and other judicial bodies the infringements of GDPR, and this must be provided by every Member State of the EU. They may also take part in any legal proceedings to ensure the GDPR is being respected and followed as required.[167]

As is stated by the GDPR's Article 58, every Member State of the EU may grant additional powers for their supervisory authorities in order for these supervisory authorities to be able to fully operate and completely investigate the issues, violations and infringments relating to the GDPR brought upon them. However, these additional powers granted to the supervisory authorities may not interfere with the Chapter VII of the GDPR, which covers topics such as the cooperation and consistency of the supervisory authorities.[168]

These supervisory authorities are must truly cooperate with each other in order to fullfil their tasks and duties set out by the GDPR. Also their decisions, and sanctions, must be consistent by nature, meaning that they have to treat different companies or organizations, which have done same infringements or violations, the same way.

The supervisory authorities will bring their findings on possible infringements or breachers of the GDPR to the national judicial authorities, unless they have been vested with the power to enforce the provisions of the GDPR themselves.[169]

All of these supervisory authorities in different EU Member states do have their own safeguards, methods and boundaries within which they has to operate, based on the Articles 51-59 of the GDPR, and they may possess additional powers granted by the national legislative bodies as long as those additional powers do not interfere with the other chapters of the GDPR or other legal framework of

167REGULATION (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 freemovement of such data, and repealing Directive 95/46/EC. General Data Protection Regulation., Article 58, Powers of the Supervisory authorities

168REGULATION (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 freemovement of such data, and repealing Directive 95/46/EC. General Data Protection Regulation.

169REGULATION (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 freemovement of such data, and repealing Directive 95/46/EC. General Data Protection Regulation., Article 58, Powers of the Supervisory authorities

the EU.[170]

The supervisory authorities exercising their powers, such as monitoring and investigating of possible violations, that are granted to them by the GDPR and the EU Member states own legislation, in harmony with the GDPR, will be subject to certain safeguard mechanisms, including effective judicial remedies in place and the due process of law,[171] which are set out by the GDPR and EU Member states own legislation.

170 GDPR-info, Art. 58 GDPR, Powers of the supervisory authorities, 2018
https://gdpr-info.eu/art-58-gdpr/
Last accessed: 10.2.2022

171 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 freemovement of such data, and repealing Directive 95/46/EC. General Data Protection Regulation., Article 58, Powers of the Supervisory authorities

3.2 Monitoring of non-compliance in the US

In the US monitoring of any non-compliance is a state legislation level matter, which means that every state has to have implemented and created their own legislation and methods on monitoring and investigating the possible non-compliances towards the privacy laws in place.[172] States which have little to no privacy laws in place usually also have less authorities monitoring these laws, as it can be seen as waste of resources, like money or man power.

It is an interesting fact that US does not actually even have any separate supervisory authorities, such as the EU has, monitoring or investigating the companies or the organizations. The US system revolves around individuals that have to bring a civil claim forward to a court in order to have the possible infringement of the privacy law investigated by the US authorities. These individuals can be awarded with compensation for any of the damages the willful or intentional non-compliance by the companies or the organizations has caused them.[173]

USA has always been seen as a police state, where police, as official authorities investigating issues or possible violations of law, has the power to do almost anything they need to do, and it is always within the law, even if sometimes it is seen as it is even above the laws that regulate their actions and methods.

As long as the police can justify their actions with the need or good for the most of the people, such allows them almost illegal searching of premises or detaining people in order to create peace to most of the people. This isn't the case with the privacy laws, as it has to come from the individuals that the states should take actions, such as investigating the claim brought forward to a court. This can be seen as a safeguard to the companies, because when the court case is filed, the companies have the possibility to enter negotiations with the plaintiffs in order to avoid court decisions and sanctions.

---

172 Judicial Remedies and Penalties for Violating the Privacy Act, The United States Department of Justice, https://www.justice.gov/jm/eousa-resource-manual-142-judicial-remedies-and-penalties-violating-privacy-act Last accessed 8.2.2022

173 Judicial Remedies and Penalties for Violating the Privacy Act, The United States Department of Justice, https://www.justice.gov/jm/eousa-resource-manual-142-judicial-remedies-and-penalties-violating-privacy-act Last accessed 8.2.2022

As the US court system in privacy law matters, such as the Privacy Act, is based on awarding the plaintiff compensation on the damages they have received, these negotiations can be seen as a way to pay someone to be silent about an issue.[174]

The lack of harmonization between the US states in the area of privacy laws allows people, as well as the companies, to do forum shopping in order to find the best state to file a claim, so that they have higher chances of winning and getting bigger compensation for the damages they have received.[175] For example states which have almost no privacy laws, are more likely to decide the case in favour of the company or organization, as if there is no law regarding to some privacy matter, how could the company or the organization investigated even have broken it in the first place.

On the other hand in states with higher level of regulation concerning the privacy of individuals, such as California where the amount of privacy laws is on the highest level of the US, the case would more likely to be decided in favour of the plaintiff, and they would be awarded certain amount of compensation,[176] which the company or organization would be required to pay, the by the court's decision.

174Judicial Remedies and Penalties for Violating the Privacy Act, The United States Department of Justice, https://www.justice.gov/jm/eousa-resource-manual-142-judicial-remedies-and-penalties-violating-privacy-act Last accessed 8.2.2022

175Paul Bischoff. Internet Privacy Laws by State: which US states best protect privacy online?, Comparitech October 23, 2019 https://www.comparitech.com/blog/vpn-privacy/which-us-states-best-protect-online-privacy/ Last accessed 8.2.2022

176Judicial Remedies and Penalties for Violating the Privacy Act, The United States Department of Justice, https://www.justice.gov/jm/eousa-resource-manual-142-judicial-remedies-and-penalties-violating-privacy-act Last accessed 8.2.2022

CONCLUSIONS

The General Data Protection Regulation overall has made the situation for natural persons, as data subjects, slightly better as companies and organizations have to be more cooperating, with the GDPR, and requests that one may make to them regarding to their personal data and how it is being used.

The right to be forgotten in the Article 17 of the GDPR, which is known also as the right to erasure, plays its own role in how people can have information relating to them removed, and whether that information is actually correct or false does not matter,[177] it will be deleted from from the data controllers or processors' data centers as it is how it is named, right to erasure of personal information.

There can be found some exceptions and limitations to the Article 17 of the GDPR, such as Article 89 which limits the possibility of a person to request certain information to be removed from the saved data by a company or an organization.[178] This limitation set out by the Article 89 of the GDPR is quite vague in its range. One could even say that it is bit too vague, as it includes a lot of possible situations where the information should be saved instead of deleted, even if it has been requested to be deleted by the data subject, such situations are the public interest, some scientific or historical research, or for statistical purposes,[179] and out of these the public interest limitation can be transferred to nearly any possible situation.

The fines and sanctions that companies receive for non-cooperation, violations or failures to fullfil GDPR requirements can vary depending on multiple factors, the severity of the infringement, the

177REGULATION (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 freemovement of such data, and repealing Directive 95/46/EC. General Data Protection Regulation.: Article 17. Right to erasure

178REGULATION (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 freemovement of such data, and repealing Directive 95/46/EC. General Data Protection Regulation.: Article 89. Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

179Sanjay Sharma, Data Privacy and GDPR Handbook. Hoboken, 2020.
Ebook available on: http://search.ebscohost.com.ezproxy.utu.fi/login.aspx?direct=true&db=nlebk&AN=2319526&site=ehost-live
Last accesssed 5.2.2022

size of the company and their world wide annual revenue from their preceding financial year. Also the cooperation with the GDPR officials has positive effect on the amount of fine that the company will receive.[180]

Monitoring the GDPR is done by allowing EU Member states to set up their own supervisory authorities which will then monitor and investigate possible violations of the GDPR. This mechanism is working quite well, as data subjects may also bring forward claims of possible GDPR violations, and have these investigated, and sanctions imposed when the supervisory authorities do find those necessary.

Even though the monitoring is mostly harmonized by the GDPR, the EU Member states have received rights to grant supervisory authorities more powers than what they would receive from the GDPR, allowing EU Member states to either take more strict or less strict stand against the possible violations of the data subjects rights.[181] These possible granted powers include, for example, more easier access to the saved data and extra methods to punish the possible violations of the GDPR, as long as these are not impairing on the effective operation of the GDPR.

The difference of legislation in the US forces individuals, as data subjects, companies and organizations to look up multiple legislations in order to see whether something is against the law, or infringing some legislation, and what kind of sanctions do these award to the plaintiffs in different states, as some states might see a data sharing to third parties as allowed practice while another state's legislation strictly prohibits such practice.

In the US all of these violations of the privacy laws are brought to the courts by individuals, who have to know the legislation and have the feeling that their rights have been violated, instead of supervisory authorities, such as the EU now has, monitoring the companies or organizations on their

180REGULATION (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 freemovement of such data, and repealing Directive 95/46/EC. General Data Protection Regulation. Article 83: General conditions for imposing administrative fines, how Article 83 works.

181REGULATION (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 freemovement of such data, and repealing Directive 95/46/EC. General Data Protection Regulation. Article 58, Powers of the Supervisory authorities

own.[182] This practice is allowing the companies and the individuals to possibly enter negotiations with each other and to avoid the court decision, which could possibly be decided in anyone's favour, and to avoid the long court times, and high costs of lawyers and courts, which benefits both the individual suing for compensation and the company or organization being sued, as they most likely can negotiate the total sum to be lower than what it would be if they had gone throught the court.

The future challenges that the GDPR, and the US Privacy laws will be facing are definately related to the rapid technological advancement, as information most likely becomes more accessible and more transparent, and even better stored in the cloud environments. The information being easier to also hide behind encryption, makes it harder to know if certain information actually has been totally deleted or not.

Artificial intelligence, and its development, will also bring its own challenges when it develops to a higher and more complex state. It will also become more difficult to read the artificial intelligence and its methods of storing and sharing information, as it could be that some day it even surpasses the human intelligence in the information sector.

Another big challenge that could happen is that countries may also introduce their own legislations that could possibly tremple the territorial scope of the GDPR[183], as now it is a possible data protection legislation to any European resident, but what would happen if a country outside of the EU decides that all the companies and organizations operating on their soil will only have to follow the legislation of the said country, and that outside legislation is not applicaple to them, even when doing business with someone from the EU.

However, the current state of the GDPR, and especially the right to be forgotten, shows that companies and organizations that do learn to comply with its somewhat complex reguirements are

182Judicial Remedies and Penalties for Violating the Privacy Act, The United States Department of Justice, https://www.justice.gov/jm/eousa-resource-manual-142-judicial-remedies-and-penalties-violating-privacy-act Last accessed 8.2.2022

183REGULATION (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 freemovement of such data, and repealing Directive 95/46/EC. General Data Protection Regulation.

the ones coming out on top, and those that are violating the GDPR are in the losing end of the game. The ones complying are seen as trending, more trustworthy and people in the area of the EU are more likely to support and use the services of those that do actually follow the legislation, as the mentality of people is that if a company breaks one law, what other laws may they be willing to break for their own absolute benefit.

The market didn't really see any change after the strict privacy regulation of GDPR was introduced,[184] and at this state of the GDPR it seems that only some practices had to be changed by companies and organizations to be sure that they do indeed comply with the GDPR. For example, they had to be more open about their data sharing policies and how the collected data is used, and also more willing to comply with the requests of the individuals or the supervisory authorites.

Right to be forgotten itself is a really straight forward regulation set out by the GDPR, only its limitations are what makes it complex, and as time passes some companies or organizations will try to find ways to avoid having to delete their own information.[185] This will most likely be done by relying on the limitations of the GDPR, or by creating complex connections for the personal information, and for other information, that the data controllers want to keep stored.

184REGULATION (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 freemovement of such data, and repealing Directive 95/46/EC. General Data Protection Regulation.

185REGULATION (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 freemovement of such data, and repealing Directive 95/46/EC. General Data Protection Regulation.