
FACULTY OF LAW
Lund University

Maricar Joy Tuazon

# To Protect Lives or Personal Data?

European Privacy Regime amidst Digitalization and Coronavirus Crisis

JAEM03 Master Thesis

European Business Law
30 higher education credits

Supervisor: Ana Nordberg
Term: Spring 2021

# ABSTRACT

The adoption of the General Data Protection Regulation proclaimed Europe's stance on the significance of the right to data privacy today whereas digital technologies have prevailed all around the globe and all spheres of our lives. Digitalization is thus a phenomenon that has ever since drawn attention from leaders and policymakers which why the Regulation along with other European privacy regimes are established with the aim to govern such technologies. Such digital guidance offered by these frameworks ultimately play a key role in overcoming crises and more complex privacy challenges, and it will most particularly indicate the future of our data. This thesis thereby looks into how data protection is impacted by two ongoing events, namely the Coronavirus crisis and accelerated digitalization, in order to answer the question of whether the European privacy regimes are capable of accomplishing its objectives, addressing privacy issues, and whether these hinder the use of digital tools to support efforts against the COVID-19.

This thesis finds that COVID-19 together with accelerated digitalization have opened an essential debate on the current data protection policies. Correspondingly, the EU and other privacy advocates have highlighted that whilst these two events are both unfamiliar territories, current data protection rules were established for that same reason, which is to prepare Europe for potential privacy challenges. Hence, the European privacy regime is exhibiting capability and flexibility to address these. In the same manner, to perceive data protection as a barrier to digital developments and COVID-19 measures is to a point erroneous because data protection authorities are reassuring through its guidelines and directives that such rules complement these kinds of situations and are set up to avoid harmful consequences of processing personal data, especially health data. The enhanced obligations such a regime imposes guarantees that organisations and agencies remain responsible in its use of digital technologies to support the battle against the COVID-19.

This thesis thereby determines that the current European privacy regime remains steadfast despite such stumbling blocks. This also conveys that although COVID-19 and accelerated digitalization have demonstrated that the right to privacy is not absolute and should hence have be considered together with the public's interest and common good, it also reveals that data protection shall all the more be preserved not only to ensure compliance or overcome privacy issues but most particularly to secure the safety of our digital future.

**KEY WORDS:** Privacy, Data Protection, Technologies, Digital, Coronavirus, Pandemic Response, Special Regime, Controller, Processor, Personal Data, Rights and Digitalization.

# PREFACE

I believe that we cannot fully understand things unless we personally experience it. Battling COVID-19 in the midst of completing this thesis has indeed given me a unique perspective on the complexity of the situation happening around us, as well as the endless opportunities offered to us by today's emerging digital technologies. I am humbled and grateful for my family, friends, colleagues, and educators for shaping me to the person I am today.

This thesis draws inspiration from each one of you who continuously support and guide me in my personal and professional journey. As this thesis represents the end of my academic voyage, my hope is that this thesis will reflect my desire to enhance tech literacy amongst our future lawyers, and that it serves as a valuable source of knowledge to its readers.

*May 26 2021*

# LIST OF ABBREVIATIONS

| | |
|---|---|
| ACP | ASSOCIATION FOR PROGRESSIVE COMMUNICATIONS |
| A29WP | ARTICLE 29 WORKING PARTY |
| EU CHARTER | CHARTER OF FUNDAMENTAL RIGHTS |
| CJEU | COURT OF JUSTICE OF THE EUROPEAN UNION |
| COVID-19 | CORONAVIRUS DISEASE |
| DMA | DIGITAL MARKET ACT |
| DPA | DATA PROTECTION AUTHORITY |
| DPR | DATA PROTECTION RULES |
| DSA | DIGITAL SERVICES ACT |
| EC | EUROPEAN COMMISSION |
| ECD | E-COMMERCE DIRECTIVE |
| EDPB | EUROPEAN DATA PROTECTION BOARD |
| EDPS | EUROPEAN DATA PROTECTION SUPERVISOR |
| EPD | E-PRIVACY DIRECTIVE |
| EU | EUROPEAN UNION |
| EUDPR | EU DATA PROTECTION RULES |
| FRA | EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS |
| GDPR | GENERAL DATA PROTECTION REGULATION |
| ICO | INFORMATION COMMISSIONER'S OFFICE |
| IMY | INTEGRITETSSKYDDSMYNDIGHET |
| OECD | ORGANISATION FOR ECONOMIC COOPERATION AND DEVELOPMENT |
| SCC | STANDARD CONTRACTUAL CLAUSE |
| TFEU | TREATY ON THE FUNCTIONING OF THE EUROPEAN UNION |
| UK | UNITED KINGDOM |
| USA | UNITED STATES OF AMERICA |
| WHO | WORLD HEALTH ORGANIZATION |

# TABLE OF CONTENT

# CHAPTER I:
# INTRODUCTION

The growing role of digital technologies is evident in our society. Many companies have also realized that businesses thrive through investing and incorporating technological innovations in their operations.[1] As technologies improve our work and day-to-day lives, it raises the question of whether the benefits these bring are worth paying with our personal information. The European Commission (hereinafter 'EC') therefore recognized digital transformations as creating new opportunities for businesses within Europe, but it also calls for stronger rules empowering individuals and their digital right.[2]

The European Union (hereinafter 'EU') thus enshrine right to privacy in multiple EU legislations such as in the Treaty of the Functioning of the European Union[3] (hereinafter 'TFEU'), European Convention on Human Rights,[4] and European Charter of Fundamental Rights[5] (hereinafter 'EU Charter'). While these legislations reflect the EU's high respect to individual's privacy, the EC realized in 1995 that a European Data Protection Directive needed to be introduced to harmonize and specifically set out minimum standards on the protection of personal data.[6]

More so in early 2012, the EU Data Protection Authorities (hereinafter 'DPA') saw the rapid development of digital technologies as requiring more governance beyond a directive which ultimately led to the birth of the General Data Protection Regulation (hereinafter 'GDPR').[7] The GDPR was adopted to symbolize the Union's stance on data privacy and security by strengthening digital rights and altering how businesses handle personal data.[8]

---

[1] Tim Zanni, 'Investment in technology Innovation' [2019] KPMG 1 <https://assets.kpmg/content/dam/kpmg/uk/pdf/2019/07/investment-in-technology-innovation.pdf> accessed January 19 2021.

[2] Council Directive 95/46/EC 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 [1995] OJ L 281/31.

[3] Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union (TFEU) [2016] OJ C202/1, article 16.

[4] European Convention for the Protection of Human Rights and Fundamental Freedoms (adopted 4 November 1950, entered into force 3 September 1953) ETS 5 (ECHR) article 6.

[5] Charter of Fundamental Rights of the European Union (adopted 2 October 2000, entered into force 7 December 2000) OJ C 326/291 (EU Charter) article 8.

[6] Ibid (n 2); Ben Wolford, 'What is GDPR, the EU's new data protection law?' (*GDPR EU*) <https://gdpr.eu/what-is-gdpr/> accessed January 18 2021.

[7] Ibid; 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 (GDPR) OJ 2016 L 119/1; Wolford (n 6); European Commission (EC), 'Commission report: EU data protection rules empower citizens and are fit for the digital age' (*EC* 2020) <https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1163> accessed January 22 2021 (Empower citizens for digital age).

[8] Ibid (n 6).

The adoption of the GDPR is thereby seen as a radical change to data protection within Europe because it plays such a necessary role of ensuring honesty within industries, as well as giving more power to individuals by protecting their personal data rights.[9] This regulation especially challenges organisations within and outside Europe for it forces them to enhance its compliance spending, especially on the lawfulness of collections or processing of data that is backed up with the consequence of high fines. No matter how organisations see the GDPR, this Regulation has become more vital today to maintaining good and consistent data security practices, and for trust on digital technologies to improve.[10]

Digital technologies are thus playing a more extensive part in our daily lives. From an organisation's point of view, the GDPR may be seen as an obstacle in utilizing emerging technologies and in providing better solutions to its customers. On the other hand, organisations can achieve much better benefits through combining full compliance and digital innovation as their business' priorities.[11] According to *Håkansson*:

> Digitalization is all about building more intimate relationships with customers by applying new technologies for ... etc. to break away from competition by serving customers faster, better, and more [accurately] than before. [The GDPR encourages these digital initiatives to implement principles such as] 'Privacy by Design' and 'Privacy by Default' to minimize data exposure and the risk of being a breach.[12]

The term digitalization is often referred to as 'the process of converting [our ways] to digital form', such as where a great sphere of 'social life [is] restructured around digital communication and media infrastructures'.[13] The many potentials that digital technologies bring has resulted in many companies embracing digitalization in its pursuit of improving companies' customer relationships, reducing operation costs yet increasing overall effectiveness and efficiency, as well as maintaining competitiveness in the

[9] Alan Calder, *EU GDPR Pocket Guide* (2edn, IT Governance Publishing 2018) 9; European Data Protection Supervisor (EDPS) 9, 'The GDPR for EU institutions: your rights in the digital era 2019' [2018] EDPS <https://edps.europa.eu/sites/default/files/publication/18-12-11_factsheet1_your_rights_in_digital_era_en_2.pdf> accessed January 17 2021.
[10] Ibid.
[11] Måns Håkansson, 'GDPR: A Driver for Digitalization' (*Axiomatics*, 2017) <https://www.axiomatics.com/blog/gdpr-driver-digitalization/> accessed January 24 2021.
[12] Ibid.
[13] European Economic and Social Committee (EESC), 'Digitalisation: challenges for Europe' [2019] EESC, 80-87; 'Digitalization' (Merriam-Webster Online) <https://www.merriam-webster.com/dictionary/digitalization> accessed January 24 2021; Jason Bloomberg, 'Digitization, Digitalization, And Digital Transformation: Confuse Them At Your Peril' (*Forbes*, 29 April 2018)<https://www.forbes.com/sites/jasonbloomberg/2018/04/29/digitization-digitalization-and-digital-transformation-confuse-them-at-your-peril/>; Måns Svensson and Others, 'Digitalization and Privacy: A systematic literature review' [2016] Lund University.

market.[14] However, the GDPR highlights that seizing these new potentials comes with the responsibility to ensure a safe and secure digital life.[15]

The endless opportunities that digitalization offers to individuals and organisations became more evident as the world experiences a global health crisis, or the Coronavirus crisis.[16] In February 2020, the World Health Organization (hereinafter 'WHO') named an infectious disease and a severe acute respiratory syndrome as Coronavirus or COVID-19.[17] The Coronavirus was classified as the most crucial global health crisis of the century that forced countries to implement strict restrictions e.g. closed borders, lockdowns, and quarantines that have resulted in economic and social downturns.[18]

The COVID-19 also forced businesses, individuals, and other industries to shift to digital form and to utilise digital technologies (e.g. smartphones, geolocation, internet of things, cloud based and AI-assisted services etc) as a tool to tame virus' spread.[19] National authorities also acknowledge the use of digital technologies in their COVID-19 response which in turn required collecting, processing, and sharing of personal data (such as health records and travel information) to track covid cases, reduce risks of infection spread, as well as to gather information to guide citizens on COVID-19 symptoms and preventive steps.[20]

As mentioned by *Ventrella,* 'the way we conceive our privacy and the importance which we attach to the protection of our personal data has been

[14] Magnus Wilson and Others, 'The implications of digitalization on business model change' [2020] Innovation Engineering CIRCLE, <https://arxiv.org/pdf/2004.08937.pdf> accessed January 23 2021; Sandra Melo 'How your company can benefit from digital transformation' (*DataScope*, 2018) <https://mydatascope.com/blog/en/how-can-your-company-benefit-from-digital-transformation/#:~:text=Business%20digitization%20reduces%20operating%20costs,business%20models%20and%20revenue%20sources> accessed January 25 2021.

[15] DigitalEurope, 'Two years of GDPR: A report from the digital industry' [2020] DE 1 <https://www.digitaleurope.org/wp/wp-content/uploads/2020/06/DIGITALEUROPE_Two-years-of-GDPR_A-report-from-the-digital-industry.pdf> January 19 2021.

[16] Laura Laberge and Others, 'How COVID-19 has pushed companies over the technology tipping point—and transformed business forever' [2020] McKinsey & Company 1 <https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/how-covid-19-has-pushed-companies-over-the-technology-tipping-point-and-transformed-business-forever> accessed January 26 2021; World Health Organization (WHO), 'Coronavirus' (*WHO*) <https://www.who.int/health-topics/coronavirus> accessed January 26 2021.

[17] WHO, 'Coronavirus' (n 16); WHO, 'Coronavirus disease (COVID-19): How is it transmitted?' (*WHO*, 2020) <https://www.who.int/emergencies/diseases/novel-coronavirus-2019/question-and-answers-hub/q-a-detail/coronavirus-disease-covid-19-how-is-it-transmitted> accessed January 27 2021; Lauren M. Sauer, 'What Is Coronavirus?' (*John Hopkins Medicine*, 2021) <https://www.hopkinsmedicine.org/health/conditions-and-diseases/coronavirus> accessed January 26 2021.

[18] Indranil Chakraborty and Prasenjit Maity, 'COVID-19 outbreak: Migration, effects on society, global environment and prevention' [2020] ScienceDirect <https://doi.org/10.1016/j.scitotenv.2020.138882> accessed January 26 2021.

[19] EC, 'Digital technologies - actions in response to coronavirus pandemic' (*DG CONNECT*, 2021) <https://ec.europa.eu/digital-single-market/en/content/digital-technologies-actions-response-coronavirus-pandemic> accessed January 28 2021.

[20] Deloitte, 'Privacy and Data Protection in the age of COVID-19 Download brochure' [2020] Deloitte 1<https://www2.deloitte.com/content/dam/Deloitte/be/Documents/risk/be-risk_privacy-and-data-protection-in-the-age-of-covid-19.pdf> accessed January 28 2021, 1-4.

heavily impacted by [COVID-19]'.[21] This health crisis has accelerated digitalization more than ever, providing us with assistance in coping up with this ground-breaking event and the high-speed shift to digital forms. However, the threats it presents to digital rights is putting the GDPR and other current data protection rules (hereinafter 'DPR') to the test.[22] Thus as the GDPR enforcement agenda persists, many have expressed concerns whether these events impede data protection efforts and realization of digital rights.[23] On the other hand, whether DPR is preventing the use of digital technologies to assist in the efforts to protect citizens' lives from COVID-19 is a question that is also widely debated.[24]

## 1.1 PURPOSE AND PROBLEM

The aim of this thesis is to examine how the current European data protection regimes address privacy issues arising from Digitalization and Coronavirus crisis in order to answer the question of whether these rules hamper the use of digital technologies in efforts to protect citizens' lives from COVID-19.

To fulfil such aim, this thesis looks into the following: *firstly*, the fundamental aims of the GDPR and relevant provisions concerning this topic, as well as what kind of rights and obligations this regulations entails; *secondly*, it looks into current digital agendas and different technologies to understand its influence on privacy; *thirdly*, it looks into the present state of data protection enforcement and compliance in light of the Covid-19 and accelerated digitization; *finally*, it examines how personal data protection is balanced with public safety by understanding the scope of exemptions and derogations rules under the GDPR.

[21] Emanuele Ventrella, 'Privacy in emergency circumstances: data protection and the COVID-19 pandemic' [2020] ERA Forum 21, 379–393.
[22] Ibid, 385; Ahmad Dhaini and Others, 'Covid-19 as accelerator of digital transformation' [2020] KPMG 1 <https://assets.kpmg/content/dam/kpmg/sa/pdf/2020/covid-19-as-accelerator-of-digital-transformation-and-the-gig-economy.pdf> accessed February 1 2021.
[23] Andrew Shindler, 'Protecting Personal Data in a Pandemic: GDPR Meets COVID-19 - Part 2' (*JD Supra, Locke Lord LLP*, 2020) <https://www.jdsupra.com/legalnews/protecting-personal-data-in-a-pandemic-39288/> accessed January 30 2021; Information Commissioner's Office (ICO) 'Data protection and coronavirus - what you need to know' (*ICO*) <https://ico.org.uk/global/data-protection-and-coronavirus-information-hub/data-protection-and-coronavirus/> accessed January 30 2021.
[24] The Organisation for Economic Co-operation and Development (OECD), 'Policy Responses to Coronavirus (COVID-19): Ensuring data privacy as we battle COVID-19' [2020] OECD <https://read.oecd-ilibrary.org/view/?ref=128_128758-vfx2g82fn3&title=Ensuring-data-privacy-as-we-battle-COVID-19> accessed February 2 2021; Amy Lambert, 'Coronavirus and the GDPR – keep calm and carry on?' (*Fieldfisher*, 2020) <https://www.fieldfisher.com/en/services/privacy-security-and-information/privacy-security-and-information-law-blog/coronavirus-and-the-gdpr> accessed January 29 2021; European Data Protection Board (EDPB) Statement on the processing of personal data in the context of the COVID-19outbreak' (Adopted on 19 March 2020); Katrin Nyman Metcalf, 'COVID-19: Health or Privacy. Do We Have to Choose?' (*RWI Blog*, 2020) <https://rwi.lu.se/blog/covid-19-health-or-privacy-do-we-have-to-choose/> accessed January 29 2021.

## 1.2 MATERIALS AND METHODOLOGY

This thesis makes use of the legal dogmatic methodology that enables an examination and analysis of the current legal frameworks to determine how the law is, or *de lege lata*. According to *Hoecke*, an important part of legal doctrinal research is the explanation of the reason and whatfores of a legal rule, principles, concepts and its structure so as to correctly interpret and apply the laws.[25] However, such methodology is not merely an explanatory discipline because it also allows for an imputation approach which means that it looks for the existence of obligations under such laws and to 'better' the law.[26] This is in accordance with the approach that this thesis uses wherein it aims to understand the rationale behind the legal frameworks, it looks into the implications and compatibility of such laws in relation to the topic at hand.

A legal dogmatic methodology includes using sources that are authorized rules.[27] This thesis thus applies EU law as its primary source for it is considered an established law embodying legislative, executive and judicial functioning.[28] Relevant international and national laws that are considered as accepted sources within the meaning of Article 38 (1) of the Statute of the International Court of Justice[29] and provisions under the Vienna Convention on the Law of Treaties[30] are also used in this thesis. According to *Hart*, such sources satisfy the (i) *rule of recognition*[31] where Member States (hereinafter 'MS') have willingly and in good faith agreed to be subject to these laws and recognizes obligations thereof (ii) and the *rule of adjudication*[32] wherein these laws enable society to determine whether a breach has occurred, and the legal remedies prescribed by such laws.[33]

Since this thesis further looks into the current legal frameworks in view of the Coronavirus crisis and accelerated digitalization, it also uses a socio-legal methodology to understand the functioning of DPR in our society and in relation to current events.[34] Such 'socio-legal study is an interdisciplinary

[25] Van Hoecke, *Methodologies of legal research: what kind of method for what kind of discipline?* (Hart Oxford, 2011) 8.
[26] Ibid, 9.
[27] Claes Sandgren, 'Är rättsdogmatiken Dogmatisk?' [2008] 118(4–5) Tidsskrift for Rettsvitenskap 650, 649–650.
[28] Herbert L A Hart, *The Concept of Law* (2nd edn, Oxford Clarendon, 1994) 94-99; Thomas MJ Möllers, *Legal Methods* (Beck and Hart Publishing, 2020) 56-66.
[29] Statute of the International Court of Justice (adopted 26 June 1945, entered into force 24 October 1945) 1 UNTS XVI
[30] Vienna Convention on the Law of Treaties (adopted 25 May 1969, entered into force 27 January 1980) 1155 UNTS 331 (Vienna Convention) Articles 1-24.
[31] Leslie Green, 'The Concept of Law Revisited' [1996] 96(6) MLR <: https://repository.law.umich.edu/mlr/vol94/iss6/15> accessed February 4 2021, 1706; YALE LAW SCHOOL 3-4.
[32] Mehrdad Payandeh, 'The Concept of International Law in the Jurisprudence of H.L.A. Hart' (2011) 21(4) EJIL 967, 985-987 and 994-995; Herbert L A Hart, The Concept of Law (2nd edn, Oxford: Clarendon 1994) 94-99.
[33] Ibid (n 28).
[34] Roger Cotterrell, 'The Sociological Concept of Law' [1983] 10(2) JSTOR 241–255, 241-242; Philippa Fogarty and Others, 'Coronavirus: How can society thrive post-pandemic?' (*BBC*, 2020) <https://www.bbc.com/worklife/article/20201021-coronavirus-the-possible-long-term-mental-health-impacts> accessed February 3 2021; OECD, 'COVID-19: Protecting people and societies' [2020] OECD <https://www.oecd.org/inclusive-growth/resources/COVID-19-Protecting-people-and-

approach to analyse the law, legal phenomenon, and relationships between these and wider society'.[35] This method thus enables an examination of both the operational aspects of laws and the procedural aspects of existing judgments, as well as to analyse the social impact of such legal frameworks.[36] Accordingly, a social legal method offers a wider perspective and closer observation on the everyday legal issues and circumstances to later determine what these mean for our society.[37] In the light of these, this thesis bases its facts and analysis upon case laws, documents, guidelines, reports, comments and opinions produced by the European Union and relevant international authorities. Additional sources such as well-worked articles, research and documents are also utilized to elaborate on the topic, and to obtain multiple and different perspectives of the subject. Such supplementary materials will most importantly provide contemporary opinions and updates on the two occurring events introduced in this dissertation

## 1.3 DISPOSITION AND DELIMITATION

This thesis is composed of five chapters: the *first chapter* gives a background and present the topic; the *second chapter* offers an general understanding of the GDPR principles, relevant rights and obligations thereof; the *third chapte*r discuss the concept of digitalization and functioning of different digital technologies; the *fourth chapter* examines the Coronavirus Crisis impacts on digitalization and GDPR enforcement; the *fifth chapte*r looks into lawful restrictions on data subjects rights and the perimeters of such; the *final chapter* analyses the different areas examined and concludes on the thesis findings.

To limit this study, it will primarily focus on GDPR and discuss the most relevant provisions thereof. Hence, other legal frameworks will solely be used to elaborate and demonstrate different perspectives on the issue. This thesis will also only provide a general description on COVID-19 disease, digital tools and its technicalities; this also means that those technologies mentioned will only be those that are most commonly brought up in digital tools and privacy discussions.

societies.pdf> accessed February 4 2021; Naomi Creutzfeldt and Others, *Routledge Handbook of Socio-Legal Theory and Methods* (Routledge, 2019) 97-107.

[35] Ministry of Education Government of India (MHRD), 'Legal Research Methodology: Socio-legal Research' [2019] MHRD <http://epgp.inflibnet.ac.in/epgpdata/uploads/epgp_content/law/09._research_methodology/04._socio-legal_research/et/8151_et_et.pdf> accessed February 4 2021, 2-6; Denis Galligan, *Law in Modern Society* (OUP 2006); Reza Banakar and Max Travers, *Theory and Method in Socio-legal Research* (Hart Publishing 2005); Glenn William Wright, 'Hart's Concept of Law: Positivist Legal Theory or Sociology?' [2010] SPP <https://www.researchgate.net/publication/262566886_Hart's_Concept_of_Law_Positivist_Legal_Theory_or_Sociology> accessed February 3 2021, 4.

[36] MHRD (n 35) 2-6; Banakar and Travers (n 35).

[37] Ibid; Hart (n 28); Max Weber, *Economy and Society* (University of California Press 1968); Robert C. Ellickson, 'Order without Law: How Neighbors Settle Disputes' [1991] Harvard University Press.

# CHAPTER II:
# THE GENERAL DATA PROTECTION REGULATION

Many organisations already anticipated the significant and agile impact that the GDPR will make in different industries before it even came into force because one of its underlying aims is to overcome divergence in privacy standards and achieve total harmonisation of DPR within the Union.[38] As aforesaid, the GDPR also encompasses the EU's extending effort to ensure the realization of the fundamental right to data privacy.[39] Hence in case *Google v CNIL*[40] concerning protection of individuals in processing of personal data and free movement of such, the Court of Justice of the European Union (hereinafter 'CJEU') highlights that the GDPR allows for data subject to declare their right to access, control, correct, restrict or remove their personal information[41] from search engine operators like Google.[42] The duty to protect these rights not only applies to establishments processing personal data within the Union as it also extends to organisations in third countries that are processing EU citizen's personal data.[43]

## *2.1 EMPOWERING CITIZENS RIGHTS*

Beyond harmonising data protection laws and standards, the GDPR's fundamental purpose is to empower citizens and increase digital rights awareness.[44] Companies and other organisations are known to thrive from collecting data from its users to improve their business operations which is why individuals are placing a great value in their personal information and

[38] Rosemary Jay, *Guide to General Data Protection Regulation* (4edn, Thomson Reuters 2017) 4; Wolford (n 6); David Bender, 'GDPR harmonization: Reality or myth?' (*IAPP* 2018) <https://iapp.org/news/a/gdpr-harmonization-reality-or-myth/> accessed February 8 2021.

[39] GDPR (n 7) Recital 1; TFEU (n 3) Article 16(1), EU Charter (n 5) article 8(1); European Union Agency for Fundamental Rights (FRA), 'Data Protection' <https://fra.europa.eu/en/data-protection#:~:text=Data%20protection%20is%20a%20fundamental,that%20we%20collect%20and%20process> accessed February 10 2021.

[40] Case C-507/17 *Google LLC v Commission nationale de l'informatique et des libertés* [2019] ECLI 257.

[41] GDPR (n 7) Articles 16 and 17 on the Right to Ratification and Erasure.

[42] Ibid (n 40) 48.

[43] Ibid; GDPR (n 7) Article 3 paras 1 and 2 Mary Samonte, 'Google v CNIL Case C-507/17: The Territorial Scope of the Right to be Forgotten Under EU Law' (*ELB*, 2019) <https://europeanlawblog.eu/2019/10/29/google-v-cnil-case-c-507-17-the-territorial-scope-of-the-right-to-be-forgotten-under-eu-law/> accessed February 9 2021; Case C-131/12 *Google Spain and Google* [2014] EU C2 317, para 60.

[44] EC, Empower citizens for digital age (n 7); I-SCOOP, 'Data subject rights under GDPR - the fundamental and contextual rights' (IS EU) <https://www.i-scoop.eu/gdpr/data-subject-rights-gdpr/> accessed February 9 2021.

consider these as an asset.[45] After the GDPR came into force,[46] the EC conducted a survey where it found that around 55 to 65 percent of social network users are aware of their digital rights and enjoy these by modifying their privacy settings or restricting cookies on visited websites.[47] Hence, the GDPR ensures not only restrict personal data processing but enable subjects to be informed of the objective of processing,[48] to access and control their data,[49] to claim compensation for damages suffered from a data breach.[50]

According to Article 29 Working Party (hereinafter 'A29WP') Guidelines:

> When initiating activities that involve processing of personal data, a controller must always take time to consider what would be the appropriate lawful ground for the envisaged processing. [Consent is one of six lawful bases under Article 6 GDPR, and it is] an appropriate lawful basis if a data subject is offered control and a genuine choice with regard to accepting or declining the terms offered or declining them without detriment.[51]

Consent is fundamentally important when processing personal data, hence it is commonly used when no other lawful bases are suitable. Nevertheless, this lawful basis mostly stresses out the necessity of processing if consent is not obtained. [52] The CJEU explained in case *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV*[53] (hereinafter 'Fashion ID) that for any processing operations to be considered justifiable, website operators and providers must each pursue a legitimate interest.*[54]* In the same manner, the

[45] Mary Kay Rizzolo, '12 Reasons Why Data is Important' [2020] CQL <https://www.c-q-l.org/wp-content/uploads/2019/12/12-Reasons-Why-Data-Is-Important.pdf> accessed February 9 2021; The Grow, 'Why Is Data Important for Your Business?' (*TGC*, 2020) <https://www.grow.com/company/about-grow> accessed February 12 2021.
[46] Melissa Gustas, 'Empowering Community Engagement with the EU's General Data Protection Regulation' (*SPP*, 2018) <https://www.socialpinpoint.com/blog/empowering-community-engagement-with-the-eus-general-data-protection-regulation/#comments> accessed February 11 2021.
[47] EC, 'Special Eurobarometer 487a Report; The General Data Protection Regulation' [2019] EC; EC, 'General Data Protection Regulation shows results, but work needs to continue' (*EC* 2019) <https://ec.europa.eu/commission/presscorner/detail/en/IP_19_4449> accessed February 12 2021; EC, 'General Data Protection Regulation: one year on' (*EC*, 2019) <https://ec.europa.eu/commission/presscorner/detail/en/IP_19_2610> accessed February 13 2021.
[48] GDPR (n 7) Articles 5 (paras 1b and c), 6 and 7.
[49] GDPR (n 7) Articles 12 and 13.
[50] Gustas (n 46); Crispin Maenpaa, 'The GDPR and 25 May 2018: The finishing-line or starting pistol for data protection compliance?' (*Fleishman Hillard,* 2018) <https://fleishmanhillard.eu/2018/05/the-gdpr-and-25-may-2018-the-finishing-line-or-starting-pistol-for-data-protection-compliance/> accessed February 11 2021.
[51] Article 29 Working Party (A29WP) Guidelines on consent under Regulation 2016/679 (adopted on 28 November 2017, as last revised and adopted on 10 April 2018) 17/EN (Article 29 on consent) pages 3-5; GDPR (n 7) articles 6 and 4 para 11; EDPB, Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak (2020); EDPB, Guidelines 03/2019 on Processing of Personal Data through Video Devices (2020).
[52] ICO, 'Lawful basis for processing' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/> accessed February 12 2021; Integritetsskyddsmyndighet (IMY), 'Lawful grounds for personal data processing' <https://www.imy.se/other-lang/in-english/the-general-data-protection-regulation-gdpr/lawful-grounds-for-personal-data-processing/> accessed February 12 2021.
[53] Case C-40/17 *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV* (Fashion ID) [2019] ECLI 629.
[54] Ibid, paras 40 and 92-97; Joined Cases C-468/10 and C-469/10 *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) Administración del Estado*

United Kingdom's (hereinafter 'UK') Information Commissioner's Office (hereinafter 'ICO') is also in the opinion that it is crucial for these actors, although not exclusively, to fully involve themselves in obtaining data and consent from data subjects to ensure that its processing activities remains in line with the lawful basis it pursues.[55] On top of that, the GDPR requires organisations to establish its law before even obtaining, processing, or sharing personal data to third parties.[56]

A lawful basis such as consent thus enhances the power of individuals over the personal data as it further gives individuals the right to rectification and erasure.[57] The right to rectification under Article 16 derives from the GDPR principle on accuracy, which gives individuals the ability to correct any information regarding them.[58] Such entails that organisations must take necessary measures in guaranteeing accuracy of information obtained from data subjects, and in removing or rectifying information that is inaccurate.[59] According to Case *2007-566*[60], the right to rectification applies to objective and factual data which means that opinions and other subjective statements are excluded.[61] Although determining whether data is accurate or not is not simple, it allows individuals to express their opinions and comments concerning their data.[62] Hence, if an organisation refuses a data subject's rectification request, it must be backed up by well-founded justification and documentation of such is in place.[63]

---

[2011] ECLI 777; IMY, 'Data controllers and data processors' <https://www.imy.se/other-lang/in-english/the-general-data-protection-regulation-gdpr/data-controllers-and-data-processors/> accessed February 23 2021.

[55] Case *Fashion ID* (n 53) paras 40 and 92 - 97; Natascha Gerlach and Others, 'CJEU Judgment In The Fashion ID Case: The Role As Controller Under EU Data Protection Law Of The Website Operator That Features A Facebook 'Like' Button' (*Mondaq*, 2019) <https://www.mondaq.com/unitedstates/data-protection/833684/cjeu-judgment-in-the-fashion-id-case-the-role-as-controller-under-eu-data-protection-law-of-the-website-operator-that-features-a-facebook-39like39-button> accessed February 14 2021.

[56] Case *Fashion ID* (n 53) para 4; Gerlach and Others (n 55); ICO (n 52) Legitimate interest; Andreas Linder, *European Data Protection Law: General Data Protection Regulation* (EU 2016) 22-23.

[57] GDPR (n 7) Articles 16 and 17.

[58] GDPR (n 7) article 5; Lydia F De la Torre, 'Right to rectification under EU data protection law' (*Medium Golden Data*, 2019) <https://medium.com/golden-data/right-to-rectification-35ec099df2fc> accessed February 13 2021; Lydia F De la Torre, 'What does "accuracy" mean under EU Data Protection law?' (*Medium Golden Data*, 2019) <https://medium.com/golden-data/what-does-accuracy-mean-under-eu-data-protection-law-dbb438fc8e95> accessed February 14 2021.

[59] Dataguise, 'Data Accuracy: GDPR Principles of Processing' (GDPR Knowledge Center) <https://www.dataguise.com/gdpr-knowledge-center/data-accuracy/> accessed February 13 2021; ICO (n 52) Right to rectification.

[60] European Data Protection Supervisor (EDPS), Opinions 29 September 2008 on the notification for prior checking from the Data Protection Officer of the European Maritime Safety Agency regarding the "Recruitment of permanent, temporary and contract agents" (Case 2008-384), 10.

[61] Ibid; EDPS, Guidelines on the Rights of Individuals with regard to the Processing of Personal Data (25 February 2014) (Rights of Individuals) 18; OECD, Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (adopted 23 September 1980, amended 11 July 2013) C(80)58/FINAL, section 13 (d); Deirdre Crowley, 'Data Processing at Work: The Right to Rectification and Erasure' (*Legal Island*, 2018) <https://www.legal-island.ie/articles/ire/features/hot-topics/2018/jan/data-processing-at-work-right-to-rectification-and-erasure/> accessed February 18 2021.

[62] EDPS (n 61) Rights of Individuals, 18; EDPS, Opinions 12 September 2011 on the updated notification concerning administrative inquiries and disciplinary proceedings within the Court of Justice of the EU (Case 2011-0806), 5; ICO (n 52) Right to rectification.

[63] ICO (n 52) Right to rectification; Rachel Finn, 'The right to rectification – clarifications from the Data Protection Commission' (*Trilateral Research*) <https://www.trilateralresearch.com/the-right-to-rectification-clarifications-from-the-data-protection-commission/#:~:text=According%20to%20Article%2016%20of,it%20is%20inaccurate%20or%20incomplete> accessed

The right to erasure under Article 17 GDPR was on the hand examined in case *GC and Others*[64] where the applicants requested for third-party links leading to sensitive information concerning them to be removed by the search engine company.[65] The CJEU explained that such a right offers individuals the right to request erasure of their personal data or 'to be forgotten'.[66] While this case examined such a right in light of freedom of information under Article 11 EU Charter and Article 15 TFEU, it nevertheless highlights that organisations have to realize an individual's right to be forgotten and restrict such right only when prescribed by law.[67] With these in mind, the GDPR's fundamental aim of empowering EU data subjects not only greatly reflects on the number of rights this Regulation offers as such rights in turn implies enhanced legal duties on organisations when processing personal data.[68]

## *2.2 ENHANCED DUTIES AND OBLIGATIONS*

As organizations develop business strategies to maintain and increase their competitiveness in the market, it includes improvement on their operations to keep up with innovations and better meet their customers' needs. This in turn necessitates gathering as much personal data from its customers.[69] Therefore, although our society can immensely and economically benefit from this development, organisations tend to focus more on profiting from these data rather than leaving out privacy protection off its priority list.[70] Therefore, the GDPR lays out duties and obligations demanding organizations care more for data subject's rights.[71] Compliance to these duties not only guarantees the protection of individuals but it also gives businesses the opportunity to

February 15 2021; EC, 'How should requests from individuals exercising their data protection rights be dealt with?' (*EC*) <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/dealing-citizens/how-should-requests-individuals-exercising-their-data-protection-rights-be-dealt_en> accessed February 25 2021.

[64] Case C-136/17 *GC and Others v Commission nationale de l'informatique et des libertés* (CNIL) [2019] ECLI 773.

[65] Ibid paras 25-27.

[66] Jure Globocnik, 'The Right to Be Forgotten is Taking Shape: CJEU Judgments in GC and Others (C-136/17) and Google v CNIL (C-507/17)' [2020] 69(4) GRUR International 380, 380-382.

[67] Ibid, 380-382.

[68] Ibid; Nadège Martin and Nilofar Moini Shabestari, 'The right to be forgotten: the CJEU sides with Google in two landmark cases' (*NRF Blog*, 2019) <https://www.dataprotectionreport.com/2019/10/the-right-to-be-forgotten-the-cjeu-sides-with-google-in-two-landmark-cases/> accessed February 19 2021; Global Freedom of Expression, 'GC, AF, BH, ED v. National Commission on Informatics and Liberty (CNIL)' (GFE) <https://globalfreedomofexpression.columbia.edu/cases/gc-v-national-commission-on-informatics-and-liberty-cnil/> accessed February 18 2021; Leo Kelion, 'Google wins landmark right to be forgotten case' (BBC News, 2019) <https://www.bbc.com/news/technology-49808208> accessed February 25 2021.

[69] Ernst and Young (EY), 'GDPR: Demanding New Privacy Rights and Obligations' [2017] <https://eyfinancialservicesthoughtgallery.ie/wp-content/uploads/2017/11/ey-gdpr-demanding-new-privacy-rights-and-obligations-1_Optimized_Optimized.pdf> accessed February 23 2021.

[70] Ibid, 6; Maurice E. Stucke, 'Is competition always good?' [2017] 1(1) JAE, 163-167.

[71] Deloitte, 'A new era for privacy: GDPR Six Months On' [2018] Deloitte LLP <https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/risk/deloitte-uk-risk-gdpr-six-months-on.pdf> 6 accessed February 27 2021.

improve customer relationships as it increases trust on controllers or processors' personal data management.[72]

### 2.2.1 CONTROLLER

Processing any data hence demands the presence of a controller and processor that '[could] be a natural or legal person, public authority, agency or other body'.[73] According to Article 4 (7) GDPR, a data controller is a legal entity which determines the purpose and means of processing. Albeit this means that the data controller has the power to influence or decide over the processing of data, such power comes with the responsibility of safeguarding lawful processing and consistent compliance.[74] This in case *Jehovah's Witnesses,*[75] the CJEU stated that the applicant, a religious community, was considered a controller as it collects and processes data for the purpose of door-to-door preaching, and to later use these as a memory aid on visited people and those to be revisited.[76]

As this activity was carried out not only by the community but also members who are involved in preaching.[77] The Court recognized in this case that the manner in which these data were collected and processed is an activity falling under the EU DPR.[78] Since the community decides on how and why these personal data are processed, it fulfils the role of a controller and must thereby comply with its data protection obligations.[79]

The CJEU further explained in case *ASNEF and FECEMD*[80] that existing EU DPR[81] while the GDPR gives an exhaustive list of lawful bases for controllers to choose from, it entails a high level of duties and increased liabilities on such parties because such a lawful basis must be appropriated and justified.[82] Controllers are moreover obliged to explicitly facilitate and accommodate data subject's rights, to implement appropriate and effective measures such

[72] Ibid; EC, 'The GDPR: new opportunities, new obligations' [2018] EU Luxembourg <https://ec.europa.eu/info/sites/info/files/data-protection-factsheet-sme-obligations_en.pdf> accessed February 20 2021;
[73] EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR (adopted 2 September 2020) Summary, 9 and 24. IMY (n 54)
[74] EDPB, Guidelines 07/2020 (n 74) para 19; White Case, *Unlocking the EU General Data Protection Regulation: A practical handbook on the EU's new data protection law* (White Case LLP 2019) Chapter 10.
[75] Case C-25/17 *Tietosuojavaltuutettu v Jehovan todistajat* (*Jehovah's witnesses)* [2018] ECLI 551, para 68.
[76] Ibid (n 75) 70-75.
[77] Ibid.
[78] Ibid.
[79] Ibid; Court of Justice of the European Union (CJEU) Press Release No 103/18 on Case C-25/17 (2018).
[80] Case *ASNEF AND FECEMD* (n 54).
[81] Bird&Bird, 'CJEU decision on dynamic IP addresses touches fundamental DP law questions' (*B&B* 2016) <https://www.twobirds.com/en/news/articles/2016/global/cjeu-decision-on-dynamic-ip-addresses-touches-fundamental-dp-law-questions> accessed February 22 2021.
[82] ICO (n 52) Controllers and processors lawful basis for processing; Lydia F De la Torre, 'Valid purposes for processing ('lawful basis') under EU data protection law' (*Medium Golden Data*, 2019) <https://medium.com/golden-data/valid-purposes-for-processing-under-eu-data-protection-law-3c1fd9f4b925> accessed February 23 2021.

as setting up policies for processing, to maintain records of processing activities to demonstrate compliance, as well as to identify and mitigate potential risks of its processing activities.[83] As the GDPR indirectly forces controllers to include personal data protection in its business priorities, the CJEU nonetheless mentions that these obligations must be acknowledged in the light of work, capabilities and power of controllers when examining data breaches cases.[84]

## 2 2.2 PROCESSOR

While a data controller also has the ability to process personal data on its own, there are instances wherein it seeks for another entity or so called data 'processor' that can carry out the processing activity on their behalf.[85] Hence, the GDPR highlights that the controller will remain responsible for its processors, however, it also sets out different yet complementary duties for data processors for lawful processing of data.[86] These sets of duties and liabilities generally impels a mandatory contract between parties that sets out requirements on the processing, guidelines, security standards and instruction from the controller that data processors need to extensively follow.[87] It is additionally the duty of data processors to maintain records of all categories of processing activities as the GDPR[88] requires such information to be consistently communicated and made available to supervisory authorities.[89]

Moreover, the A29WP[90] pointed out that delegation of responsibilities in terms of processing data may imply some degree of discretion on processors to choose suitable technical, security and organizational measures to be implemented to best serve the controller's interests and fulfil its contractual duties.[91] Yet in guaranteeing its compliance with data protection obligations, data processors are obligated to take a much more cautious approach on accepting the responsibilities of processing data from controllers, as well

[83] Linder (n 56) 41-42; Gerlach and Others (n 55).
[84] Ibid. Google Spain (n 3) [38]; Case *GC and Others v CNIL* (n 65).
[85] GDPR (n 7) Article 28; EDPB, Guidelines 07/2020 (n 74) Summary, 9 and 24; IMY, 'Data controllers and data processors' (n 54).
[86] Ibid; I-SCOOP, 'What is a data processor and what are the duties of a data processor under the GDPR?' <https://www.i-scoop.eu/gdpr/data-processor-gdpr/> accessed March 2 2021.
[87] Ibid. GDPR (n 7) Article 29; Linder (n 56) 44; TermsFeed, 'GDPR Data Processor Requirements' <https://www.termsfeed.com/blog/gdpr-data-processor-requirements/#Data_Processor_Contracts_Playing_By_The_Rules> accessed February 28 2021; A29WP, Opinion 1/2010 on the concepts of 'controller' and 'processor' (adopted on 15 February 2010) 00264/10 WP 169 (Article 29 on controller and processor) 25-30.
[88] GDPR (n 7) Article 30; Debbie Heywood, 'Obligations on data processors under the GDPR' (*GDH*, 2016) <https://globaldatahub.taylorwessing.com/article/obligations-on-data-processors-under-the-gdpr> accessed March 2 2021.
[89] GDPR (n 7) Article 30 (2); DataStreams IO, 'GDPR Obligations on data processors' [2019] DSIO.
[90] Article 29 on controller and processor (n 87) 25-30.
[91] Ibid, 25; Case C-210/16 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH* [2016] ECLI 388.

passing such obligations to sub-processors because the GDPR now sets out direct liability on processors.[92]

Such direct liability enables data subjects to bring claims against processors if non-compliance to its contractual and GDPR obligations can be displayed,[93] and to claim compensation from processors for damages suffered.[94] These demonstrates that although controllers remain at first hand responsible for determining processing purposes and facilitating data subject rights such as under Article 12 to 23 GDPR, it doesn't mean that processors can escape mishandling personal data because not only do they have obligations on their own but they are also demanded to actively support controllers in responding to data subjects requests.[95]

### 2.2.3 JOINT CONTROLLERS

Whereas it is explained above that a processor and controller have distinguishing roles and obligations when conducting data processing activities, there are also circumstances where there is joint controllership. This signifies that a processor surpasses the assigned instructions and takes part in determining objectives of the data processing.[96] In an earlier case, the CJEU similarly examined an online retailer, *Fashion ID,* that the applicant claimed to have violated the EU law through including a like button on their website that transmits data subject's data to servers owned by Facebook. The Court explained that Facebook and *Fashion ID* have joint controllership because the embedded plug-in enables the transmission of personal data of *Fashion ID*'s web visitors to Facebook which in turn means that Fashion ID have a decisive power on the collection and disclosure of such data.[97]

Apart from clarifying the notion of joint controllership, this case went on by examining the division of responsibilities in processing activities that involve joint controllership.[98] Accordingly, the finding that *Fashion ID* and Facebook share controllership does automatically indicate equally shared duties

[92] GDPR (n 7) Article 82(1-2); Alexander Brown, 'Impact on data processors' (*Simmons & Simmons*) <https://www.simmons-simmons.com/en/features/european-data-protection-regulation/ck0zgbujqdfiu0b49om90f11g/european-data-protection-regulation-impact-on-data-processors> accessed February 26 2021; Brendan Van Alsenoy, 'Liability under EU Data Protection Law' [2016] JIPITEC 271, 278.
[93] White Case (n 74) Chapter 11.
[94] GDPR (n 7) Article 82; Alex Bussche and Paul Voigt, 'GDPR Processor Obligations' (*Taylor Wessing*, 2020) <https://www.taylorwessing.com/en/insights-and-events/insights/2020/08/gdpr-processor-obligations> accessed March 2 2021.
[95] Bussche and Voigt (n 94).
[96] GDPR (n 7) Article 26.
[97] Case *Fashion ID* (n 53) 8 and 5/11; René Mahieu and Joris van Hoboken, 'Fashion-ID: Introducing a phase-oriented approach to data protection?' (*ELB*, 2019) <https://europeanlawblog.eu/2019/09/30/fashion-id-introducing-a-phase-oriented-approach-to-data-protection/> accessed March 1 2021.
[98] Ibid; IApp, 'CJEU releases judgement on Fashion ID' (*IAPP*, 2019) <https://iapp.org/news/a/cjeu-rules-websites-responsible-for-data-processing-via-facebook-like-button/> accessed March 3 2021.

because such joint control might only take place in certain processing activities – this e.g. means that other stages of processing may only be conducted by one of the controllers or may only have access to personal data to a certain degree.[99] Although the case does not dive deeper into joint controllers' obligations, the CJEU explicitly stresses that website operator's bear the duty to obtain consent from data subjects before data collection, and clearly inform its identity and purposes of processing.[100] For organisations entering a joint controllership it would thus be crucial to establish respective duties prior to any processing activity to ensure GDPR compliance.

To conclude, the GDPR signifies the Union's attempt to bring together companies and customers closer through trust within Europe. This Regulation empowers data subjects' rights over their data by ensuring that individuals remain at the centre and a priority for organisations in their business operations. Similarly, the GDPR embodies an extraterritorial jurisdiction to extend data protection of EU citizens by further demanding organisations outside EU to take adequate measures in protecting personal data and encouraging them to level its standards according to the GDPR.[101] Such elements of the GDPR are detrimental not only for protection of individuals but also in shaping and promoting a safer digital world that goes beyond the European borders.

[99] Tobias Bräutigam,'CJEU Fashion ID Case: Thumbs down to Facebook's' (B&B, 2019) <https://www.twobirds.com/en/news/articles/2019/global/cjeu-fashion-id-case-thumbs-down-to-facebook%27s-like-feature> accessed March 4 2021.

[100] CJEU, Press Release No 99/19 on Case C-40/17 (2019); Maarten Stassen and Heidi Waem, 'What we can learn about joint controllership from the CJEU Fashion ID ruling' (*Crowell Moring*, 2019) <https://www.crowelldatalaw.com/2019/08/what-we-can-learn-about-joint-controllership-from-the-cjeu-fashion-id-ruling/#page=1> accessed March 3 2021; Gerlach and Others (n 55).

[101] Kriangsak Kittichaisaree and Christopher Kuner, 'The Growing Importance of Data Protection in Public International Law' (*EJIL*, 2015) <https://www.ejiltalk.org/the-growing-importance-of-data-protection-in-public-international-law/> accessed March 4 2021.

# CHAPTER III:
# DIGITAL TRANSFORMATIONS

Our world heavily relies on digital approaches to create new opportunities for businesses and transform our living standards.[102] Today, digital transformation is one of those that are 'profound[ly changing and accelerating] business activities, processes, competencies, and models'.[103] Digital transformation is a concept that is as complex as its potential, yet it allows us to explore and use technologies to our benefit and to meet our needs. Hence, this phenomenon has driven different industries to aim for digitalization and integrate technologies into all areas of its business operations and delivery.[104]

On the other hand, such transformations do not solely come with benefits as it additionally brings challenges on current data protection regimes. That is why the EDPS released a Digital Strategy in 2020, also known as *Shaping a Safer Digital Future,* whose objective is to tackle challenges and negative impact that digitalization presents on individual rights. The EDPS delineates in its strategy that:

> The increased dependency on data and technology amplifies the pre-existing conditions of our digital ecosystem, including the concentration of market power, information asymmetries, disinformation, manipulation, data breaches and platform dominance.[105]

This 2020 Digital Strategy[106] therefore reiterates that digital transformations also have the tendency of impeding individual rights and freedoms because these technologies are primarily driven by personal data that organisations may exploit and profit from.[107] This not only negatively affects the internal market but also restricts consumers' choices.[108]

---

[102] Enrique Dans, 'Innovation, the Future of Society and People' [2019] Medium <https://www.enriquedans.com/wp-content/uploads/2019/11/Indra_Dans_ing.pdf> accessed March 10 2021.
[103] Peter M. Bican and Alexander Brem, 'Digital Business Model, Digital Transformation, Digital Entrepreneurship: Is There A Sustainable "Digital"?' [2020] MDPI <https://www.researchgate.net/publication/342580682 Digital Business Model Digital Transformation Digital_Entrepreneurship_Is_There_A_Sustainable_Digital/fulltext/5efbe5e5299bf18816f5f3c1/Digital-Business-Model-Digital-Transformation-Digital-Entrepreneurship-Is-There-A-Sustainable-Digital.pdf> accessed March 7 2021, 3.
[104] The Enterprisers Project, 'What is digital transformation?' (*Red Hat*, 2016) <https://enterprisersproject.com/what-is-digital-transformation> accessed March 7 2021.
[105] EDPS, Shaping a Safer Digital Future: The EDPS Strategy 2020 - 2024 (2020) EU (2020 Digital Strategy); EDPS, 'Annual Report 2020' [2021] EU.
[106] Ibid.
[107] Ibid.
[108] Ibid.

Since it was aforementioned that the GDPR enforcement is just in its third year, a number of digital technologies today were e.g. created by tech giants and designed without the Regulation in mind. Therefore, data protection regimes needed not only to guide digital innovations but to also alter the way these technologies are utilized and implemented in business operations. The GDPR with the help of national DPA are thus two key elements because these represent and uphold data subjects' interests, as well as their digital rights under the existing EU DPR.[109]

In the time of rapid shift to digital forms, such established Digital Strategy therefore demands solidarity from MS to preserve the values and fundamental rights to privacy, and disregard business operations that damage the trust in digital technologies.[110] Such solidarity also requires active cooperation in enforcing data protection policies and agendas that pushes organisations to embed protection of personal data in their digital technologies.[111] This Digital Strategy should nevertheless enable digitalization work both for citizens and companies because such frameworks will dictate how societies capture the complexity and challenges that accompany these digital technologies.[112]

## *3.1 DIGITAL AGENDA AND POLICIES IN PROCESS*

Prior to the 2020 Digital Strategy, the EC launched a *Digital Agenda for Europe*[113] in 2010 as one of the first flagship initiatives to safeguard the fairness, transparency and security of the digital environment, [114] and to fully unfold potentials of these technologies to enable for positive and smart growth.[115] The EC believes that this Digital Agenda will widen and streamline the use of digital technologies to address current challenges and improve

[109] Ibid, 4-8; Frances Burwell, 'First privacy, now data: The EU seeks a managed digital space' (*Atlantic Council*, 2020) <https://www.atlanticcouncil.org/blogs/new-atlanticist/first-privacy-now-data-the-eu-seeks-a-managed-digital-space/> accessed March 6 2021.
[110] EU, Shaping a safer digital future (n 106) 4-9; Hogan Lovells, 'Shaping Europe's Digital Future – EU publishes its draft Digital Services Act' (*JD Supra*, 2020) <https://www.jdsupra.com/legalnews/shaping-europe-s-digital-future-eu-75285/> accessed March 10 2021; Burwell (n 109).
[111] EC, 'A Europe fit for the digital age' <https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_en#:~:text=The%20EU%27s%20digital%20strategy%20aims,this%20Europe%27s%20%E2%80%9CDigital%20Decade%E2%80%9D> accessed March 13 2021.
[112] Katrin Rohmann and Others, 'Digital Transformation in the EU 2035 A Glimpse into the Future' [2019] 7 Deloitte, 3-7; Marguerit Lane, 'Regulating platform work in the digital age' [2020] 1 OECD <https://goingdigital.oecd.org/toolkitnotes/regulating-platform-work-in-the-digital-age.pdf> accessed March 13 2021.
[113] EC, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions A Digital Agenda for Europe (2010) COM(2010)245 (EU Digital Agenda).
[114] European Parliament (EP), 'Digital Agenda for Europe' [2021] EU EP <https://www.europarl.europa.eu/ftu/pdf/en/FTU_2.4.3.pdf> accessed March 11 2021.
[115] Ibid.

citizens' lives through e.g. better health care, safer transport solutions, cleaner environment, and easier access to public service.[116]

This Agenda also enables the EU to be a frontrunner on the 'data-agile economy' for the next five years whilst also maintaining respect for European values.[117] Apart from existing data regulations (e.g, EPD[118], ECD, Open Data Directive[119] and GDPR), the EU thus continuously develops guidelines and communications to complement the current privacy regimes.[120] Accordingly, this instrument has the goal to foster data governance yet it is through data protection legislations that an individual's digital privacy can be fully preserved.[121]

For these reasons, the EU proposes the adoption of Digital Services Act (hereinafter 'DSA') that will further expand data protection standards and reinforce governance of digital tools than what GDPR has been created.[122] As stated by *Blankertz* and *Jausch*, 'whereas the GDPR harmonized and, in many countries, raised data protection standards, the DSA is not limited to one specific policy field but aims to establish a comprehensive framework for how "digital services" operate in Europe'.[123] The DSA will thus impose greater responsibility on digital platforms such as what is published, advertised and overall content of their websites and online channels. Online service providers or digital marketplaces such as Amazon, Facebook, App Store etc will thus have to implement extensive and good security practices on their platforms and maintain an open and accessible online world for all.[124]

---

[116] Ibid; HealthManagement, 'European Commission Announces Digital Agenda for Europe' [2010] 10(3) HM <https://healthmanagement.org/pdf/article/european-commission-announces-digital-agenda-for-europe> accessed March 16 2021.

[117] Association for Progressive Communications (APC), 'The EU's plans for its digital future' (*Apc News*, 2020) <https://www.apc.org/en/news/eus-plans-its-digital-future> accessed March 13 2021.

[118] Council Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L 201 (EPD).

[119] Council Directive 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information [2019] OJ L 172.

[120] APC (n 117); EC, 'Foreign Policy' (*EC*, 2021) <https://digital-strategy.ec.europa.eu/en/policies/foreign-policy> accessed February 28 2021; EC, 'Europe 2020: A European strategy for smart, sustainable and inclusive growth' [2020] COM/2010/2020 final (Europe 2020).

[121] Ibid.

[122] APC (n 117); Aline Blankertz and Julian Jaursch, 'How the EU plans to rewrite the rules for the internet' (*Brookings*, 2020) <https://www.brookings.edu/techstream/how-the-eu-plans-to-rewrite-the-rules-for-the-internet/> accessed March 11 2021; EC, 'The Digital Services Act: ensuring a safe and accountable online environment' (*EC*, 2020) (A safe and accountable online environment) <https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en> accessed March 16 2021; EP, 'Digital Services Act: Legislative train schedule' (*EP*, 2021) (Legislative Train Schedule) <https://www.europarl.europa.eu/legislative-train/api/stages/report/current/theme/a-europe-fit-for-the-digital-age/file/digital-services-act> accessed March 15 2021; Alice Tidey and Others, 'Digital Service Act: EU vows to 'put order into chaos' with tech laws' (*EuroNews*, 2020) <https://www.euronews.com/2020/12/15/digital-services-act-brussels-unveils-landmark-plans-to-regulate-tech-companies> accessed March 16 2021.

[123] Ibid.

[124] Svenskt Näringsliv, 'Position Paper: Digital Services Act' [2020] SN 1.

The DSA also goes beyond the rules set out in the E-Commerce Directive (hereinafter 'ECD') because it is intended to set a higher standard that in turn means that it will ultimately replace and expand the ECD. Similarly, the DSA is an effort by the EU to adjust the current ECD rules to the currently changing digital world whilst safeguarding specific human rights (e.g. freedom of information and expression[125]).[126] On the other hand, DSA will have major American tech companies as it subjects; therefore, it could be said that DSA is as a positive aftermath of *Schrems*[127] cases for its influence on EU's legislative efforts to intensify European's digital rights.[128]

The case of *Maximillian Schrems v Data Protection Commissioner*[129], also known as *Schrems* case*,* involves an applicant who is an Austrian lawyer and privacy advocate. Mr. Schrems complained about Facebook's data collection and transfer of data to the United States of America (hereinafter 'USA').[130] Albeit this case unfolding the divergence between USA[131] and EU privacy laws, it sheds light on data transfers to third countries which the GDPR only permits under certain conditions. This first *Schrems* case outcome is widely debated because the CJEU invalidated the Safe Harbor[132] arrangement between EU and US as it was in the opinion that such a framework does not adequately safeguard the protection of EU citizens personal data.[133]

[125] EU Charter (n 5); ECHR (n 5) Article 10.
[126] Ibid (n 122); APC (n 117); Svenskt Näringsliv (n 124); Emma Llanso, 'The DSA: An Opportunity to Build Human Rights Safeguards into Notice and Action' (*Medium Global Network Initiative* (GNI) 2020);
[127] Case C-362/14 *Maximillian Schrems v Data Protection Commissioner* (Schrems I Case) [2015] ECLI C 650.
[128] EDPS, Opinions 10 February 2021 on the Digital Services Act and the Digital Markets Act (2021) EDPS/2021/02 (Opinions on the DSA and DMA); Eileen Kannengeiser and Jörn Fleck, 'Europe's new legislative proposals mark a big 'first move' on tech-market power' (*Atlantic Council*, 2020) <https://www.atlanticcouncil.org/blogs/new-atlanticist/europes-new-legislative-proposals-mark-a-big-first-move-on-tech-market-power/> accessed March 18 2021; Samuel Stolton, 'Digital Brief: Schrems 3? Clearview AI furore, EU facial recognition ban' (EurActiv, 2020) <https://www.euractiv.com/section/digital/news/digital-brief-schrems-3-clearview-ai-furore-eu-facial-recognition-ban/> accessed March 13 2021; Bart Van den Brande, 'The future Digital Services Act and Digital Markets Act in a nutshell' (*Sirius.Legal*, 2021) <https://siriuslegaladvocaten.be/en/the-future-digital-services-act-and-digital-markets-act/> accessed March 16 2021.
[129] Simplify, 'You've put GDPR to bed, then you wake up with Schrems II' (*Simplify*, 2020) https://symplify.com/blog/youve-put-gdpr-to-bed-then-you-wake-up-with-schrems-ii/?utm_campaign=schrems&gclid=CjwKCAiAg8OBBhA8EiwAlKw3kq_XyTlStHyFtxfPHgSpVyuzQ4iZre89vPOu_euvAQvn0hHzyCSH9BoCo6wQAvD_BwE> accessed March 15 2021; EPIC, 'Max Schrems v. Data Protection Commissioner' (*Epic.Org*) <https://epic.org/privacy/intl/schrems/> accessed March 20 2021.
[130] Simplify (n 129).
[131] USA Privacy Act of 1974 (approved and effective 31 December 1974) PL 93-579; US Department of Justice, *Guide to the Freedom of Information Act* (DOJ FOI 2020).
[132] Schrems I (n 127); Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce [2000] OJ L 215.
[133] Schrems I (n 127), paras 73-78; Global Freedom of Expression, 'Schrems v. Data Protection Commissioner' (*GFE Columbia University*, 2020) <https://globalfreedomofexpression.columbia.edu/cases/schrems-v-data-protection-commissioner/> accessed March 23 2021; Joshua P. Meltzer, 'The Court of Justice of the European Union in Schrems II' (*Brookings*, 2020) <https://www.brookings.edu/research/the-court-of-justice-of-the-european-union-in-schrems-ii-the-impact-of-gdpr-on-data-flows-and-national-security/> accessed March 20 2021.

Following this case, the EU and USA attempted to come together and replace Safe Harbor with a Privacy Shield.[134] This Privacy Shield intended to ensure consistency of data transfers to the USA through Standard Contractual Clause (hereinafter 'SCC').[135] Not too long after such framework was established, Maximilian claimed that Facebook's use of SCC to transfer EU citizens' data to the USA remains to be an inadequate protection thus challenging this in the *Schrems II*[136] case.[137] This case followed a similar path as *Schrems I* where the Court invalidated Privacy Shield and explained that:

> The GDPR must be interpreted as meaning that the appropriate safeguards, enforceable rights and effective legal remedies required by those provisions must ensure that data subjects whose personal data are transferred to a third country pursuant to standard data protection clauses are afforded a level of protection essentially equivalent to that guaranteed within the [GDPR].[138]

The rapid shift to digital form presents threats on data protection because many organisations may involve transferring and processing personal data outside the Union. Hence, the *Schrems* case' exhibits that the GDPR demands organisation to assess that any data transfers beyond the Union will uphold the same level of protection provided in the GDPR, through contractual clauses or considering national laws of the recipient.[139]

Digital technologies may have enabled free movement and better data flows but also enabled new opportunities for cybercriminals to infiltrate data systems and maliciously steal unencrypted personal data and credentials.[140] The outcomes of *Schrems* cases have interrupted businesses to some degree because the decision implicates reconsiderations of other mechanisms that safeguard personal data transfer with third parties or countries. Although this may be an eye-opener for organisations, the EU may nevertheless need to

---

[134] Privacy Shield Framework, 'Privacy Shield Program Overview' <https://www.privacyshield.gov/Program-Overview> accessed March 23 2021.

[135] Shreya Tewari, 'Schrems II: A brief history, an analysis and the way forward' (*Inforrm*, 2020) <https://inforrm.org/2020/07/23/schrems-ii-a-brief-history-an-analysis-and-the-way-forward-shreya-tewari/> accessed March 21 2021.

[136] Case C-311/18 *Data Protection Commissioner v Facebook Ireland Ltd* (Schrems II) [2020] ECLI 559; EP, 'The CJEU judgment in the Schrems II case' [2020] EPRS PE 652 073.

[137] Ibid (n 136); Simplify (n 129); Marie McGinley, 'Schrems II Judgement: Standard Contractual Clauses' (*Eversheds Sutherland*, 2020) <https://www.eversheds-sutherland.com/global/en/what/articles/index.page?ArticleID=en/global/ireland/schrems-ii-judgement-170720> accessed March 21 2021; Christopher Kuner, The Schrems II judgment of the Court of Justice and the future of data transfer regulation (*ELB*, 2020) <https://europeanlawblog.eu/2020/07/17/the-schrems-ii-judgment-of-the-court-of-justice-and-the-future-of-data-transfer-regulation/> accessed March 21 2021.

[138] Schrems II (n 136) para 105; Tewari (n 135).

[139] Kuner (n 138); Nigel Cory and Others, 'Schrems II': What Invalidating the EU-U.S. Privacy Shield Means for Transatlantic Trade and Innovation' (*ITIF*, 2020) <https://itif.org/publications/2020/12/03/schrems-ii-what-invalidating-eu-us-privacy-shield-means-transatlantic> accessed March 28 2021.

[140] Dagmar Rosenbrand and Others, *Risk Classification of Data Transfer in Medical Systems. Computer Safety, Reliability, and Security* (Springer 2015) 243-251.

establish a supplementary and concrete framework that will provide adequate protection for personal data transferred to third parties or countries.[141] Accordingly, such future legal framework would need to carefully take into account the fundamental right to data protection alongside the aim of the EU to 'benefit from data-driven innovation, strengthen trade between countries in a growing range of digital and digitally enabled goods and services, and expand consumers' access to a growing variety of goods and services'. [142]

The EC thereby plans to complement existing data regulations and the DSA with another framework called Digital Market Act (hereinafter 'DMA').[143] The EDPS acknowledges the DMA proposal because it believes that digital markets and economies will at most flourish if the policies concerning competition, consumer protection and data rights protection are conceived as three interlinked areas rather than conflicting.[144] The principal objective of DMA is thereby to build digital space upon the EU fundamental rights, as well as to protect the internal market and consumers from giant platform services like Amazon and App stores.[145]

To put into context, both DSA and DMA intend to establish consistency between the different digital service rules within and outside Europe in order to limit the economic powers these tech giants hold or so called 'gatekeepers'.[146] Notwithstanding, such future digital policies should affirm that the digital well-being of individuals remains in centre whilst promoting societal and economic growth.[147] These upcoming policies will have to be regarded rapidly and diligently enough to cope up with the rapid digital transformations.[148]

---

[141] Cory and Others (n 139).

[142] Ibid; Case C-101/01 *Bodil Lindqvist* [2003] ECR I-12971; Diane Rowland and Others, *Information Technology Law* (4edn, Routledge 2012) 162-164; Daria Rutecka, 'Schrems II – Follow-up On New Protective Measures For Safe Data Transfers' (*Mondaq*, 2020) <https://www.mondaq.com/data-protection/1012794/schrems-ii-follow-up-on-new-protective-measures-for-safe-data-transfers> accessed March 24 2021.

[143] EDPS, Opinions on the DSA and DMA (n 128).

[144] EDPS, Opinions on the DSA and DMA (n 128); EP, Digital Agenda for Europe (n 114); EC, 'The Digital Markets Act: ensuring fair and open digital markets' (2020) <https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en> accessed March 24 2021.

[145] Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Proposal for DMA) COM(2020) 842 final, 11 and 23; EC, 'The Digital Services Act package' (2021) <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package> accessed March 22 2021.

[146] EC, Proposal for DMA (n 146) 3; Van den Brande (n 129); Aline Blankertz and Julian Jaursch, 'What the European DSA and DMA proposals mean for online platforms' (*Brookings*, 2021) <https://www.brookings.edu/techstream/what-the-european-dsa-and-dma-proposals-mean-for-online-platforms/> accessed March 28 2021; Rohmann and Others (n 112); EC, 'Europe fit for the Digital Age: New online rules for businesses' <https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment/europe-fit-digital-age-new-online-rules-businesses_en> accessed March 25 2021.

[147] OECD, 'Going Digital: Shaping Policies, Improving Lives' [2003] OECD <https://www.oecd.org/going-digital/going-digital-synthesis-summary.pdf> accessed March 27 2021; EC, 'Data policies and legislation - 'Timeline' (2020) <https://ec.europa.eu/digital-single-market/en/data-policies-and-legislation-timeline> accessed March 30 2021.

[148] Ibid (n 151); Chris Ruff, 'A Stronger Digital Europe' [2020] DigitalEurope <https://www.digitaleurope.org/wp/wp-content/uploads/2019/02/DIGITALEUROPE-%E2%80%93-Our-Call-to-Action-for-A-STRONGER-DIGITAL-EUROPE.pdf> accessed March 28 2021.

Digitalization demands not only for EU MS to come together but for neighbouring and third countries' cooperation in promoting the EU's digital agenda and strategy, as well as to unlock the benefits of digital transformations.[149] Driving these digital technologies to the right course can be done through identifying potential effects and challenges it will impose and from there, prepare and protect our societies through policies that can tackle the next digital chapter.[150] Hence current digital strategies, agendas and policies in process will not only allow us to create robust but flexible frameworks but it will also determine the next era we will be living in.[151] In order to do so privacy regulators and advocates need to gain a clearer picture of what these digital technologies are, how these function and what effects these tools have on the right to privacy to truly overcome potential stumbling blocks in its efforts to shape a safer digital world.

## *3.2 DIFFERENT DIGITAL TECHNOLOGIES*

The digital agenda is a proclamation of enhanced efforts to promote effective but secure digital technologies. As part of such its digital action plans, the EC reiterates that digital transformations should be about empowerment and emancipation.[152] For this to be possible, an opportunity to enhance digital literacy and skills should be offered to not only policymakers, but also European citizens because these technologies are an integral part of life.[153] Such a goal to equip leaders and individuals with digital competences thereby lies at the heart of these referred agendas.[154] This is because digital technologies fundamentally serve the purpose of increasing effectiveness and efficiency on how we work, operate and communicate, as well as to develop our skills.[155] Hence, it sequentially demands investing in people and

[149] Rohmann and Others (n 112) 12; EC, Foreign Policy (n 121); EC, 'Promoting Europe's interest and protecting European Values in the Global Digital Transformation' [2019] <https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=61697> accessed March 28 2021.
[150] EDPS, 'Shaping a Safer Digital Future: a New Strategy for a New Decade' (2021) <https://edps.europa.eu/press-publications/publications/strategy/shaping-safer-digital-future_en> accessed March 30 2021.
[151] Rohmann and Others (n 112) 3-7; Lane (n 112); EC, 'EU Budget for the Future' [2018] <https://euagenda.eu/upload/publications/untitled-199893-ea.pdf> accessed March 30 2021.
[152] EU Digital Agenda for Europe (n 114) 24–26.
[153] Ibid.
[154] EC, 'Measuring Digital Skills across the EU: EU wide indicators of Digital Competence' (2014) <https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=5406> accessed April 3 2021.
[155] Radhika Kapur, 'Significance of Digital Technology' [2018] 3-17; Caroline Paunov and Sandra Satorra, 'How are digital technologies changing innovation?' [2019] OECD <https://www.researchgate.net/profile/Caroline-Paunov/publication/334593576_HOW_ARE_DIGITAL_TECHNOLOGIES_CHANGING_INNOVATION/links/5d337e8a92851cd04678a9b6/HOW-ARE-DIGITAL-TECHNOLOGIES-CHANGING-INNOVATION.pdf> accessed April 4 2021; Sabine Verheyen, 'Why investing in digital literacy now will secure the future of the EU' (*TPM*, 2020) <https://www.theparliamentmagazine.eu/news/article/why-investing-in-digital-literacy-now-will-secure-the-future-of-the-eu> accessed April 4 2021.

improving their understanding of what these technologies are and its functions. [156]

According to the EU Digital Literacy High-level Expert Group, 'digital literacy is increasingly becoming an essential life skill and the inability to access or use ICT has effectively become a barrier to social integration and personal development' which signifies that enhancing digital literacy and privacy rights thereof is an essential for the EU to benefit from these technologies not only economically but also socially.[157] This may also support EU DPR compliance because it further encourages EU citizens to facilitate privacy efforts by becoming 'agents of social change' and playing an active role in enforcing their data protecting rights all the more.[158] Most importantly, individuals will have empowered abilities to understand how digital technologies impact their right to privacy and to protect themselves from organisations who may unlawful and for malicious purposes process their data.

### 3.2.1 INTERNET AND TELECOMMUNICATIONS

As aforesaid, digital technologies are undoubtedly serving its purposes because the internet and telecommunication technologies have introduced infinite advantages such as receiving information. According to *Peckham*, the internet can be described as a global network which provides information and communication alternatives for users. On the other hand, telecommunication is a wider terminology that entails an exchange of information (e.g data, video, text etc) and circumscribes different technologies such as fiber optics, radio, internet and other transmitted communication.[159]

One of the most common examples of internet technology is a search engine. This digital tool allows us to type a query in a search box and find multiple information in just seconds. Such a search engine contains a database of information, as well as algorithms that finds and evaluates the query to deliver

[156] SchengenVisaInfo, 'Over 15% of Youngsters in EU Demonstrate Insufficient Digital Skills' (*SVI*, 2020) <https://www.schengenvisainfo.com/news/report-over-15-of-youngsters-in-eu-demonstrate-insufficient-digital-skills/> accessed April 3 2021; Burkhard Schäffer, 'The Digital Literacy of Seniors' [2007] 2(1) Universität der Bundeswehr.
[157] EC, 'DG Information Society and Media at a Glance' [2006]; Beverley Bunker, 'A Summary of International Reports, Research and Case Studies of Digital Literacy' [2010] NZCS <https://itp.nz/files/201001%20Digital%20Literacy%20Research%20Report.pdf> accessed March 29 2021, 13.
[158] Philipp K. Masur, 'How Online Privacy Literacy Supports Self-Data Protection and Self-Determination in the Age of Information' [2020] 8(2) COGITATIO 258–269; EC, 'Digital Education Action Plan (2021-2027)' (2020) <https://ec.europa.eu/education/sites/default/files/document-library-docs/deap-communication-sept2020_en.pdf> accessed March 29 2021.
[159] Brittany Peckham, 'Internet vs telecommunications: difference that matters for users' rights' (*Valicom*, 2019) <https://www.valicomcorp.com/blog/2019/1/28/internet-vs-telecommunication-services-differences-that-matter-for-users-rights#:~:text=The%20internet%20is%20a%20global,and%20data%2C%20using%20electronic%20devices> accessed April 3 2021.

relevant information.[160] Beyond that, it is worth noting that search engines collect the users search logs, date, locations and IP addresses to deliver more accurate results. While this digital tool helps to organize the internet and for individuals to obtain vast amounts of information in no time, it is a threat to privacy as the data it collects are some of the most personal and sensitive data on users (e.g passwords and bank credentials).[161]

The internet additionally offers possibilities to organisations to improve their internal communications through sharing and managing company's data activities through solutions such as the 'cloud'.[162] According to *Microsoft*, this is especially beneficial for organisations that have a huge number of employees and operate in different locations because it grants them to save e-documents to remote databases and retrieve these upon request, as well as to move and transfer data to servers everywhere in the world. [163]

However, the manner in which cloud technologies allow for dispersal of data beyond national or European boundaries poses data protection issues such as seen in *Schrems* case because privacy as personal data is stored and processed under multiple jurisdictions.[164] The advanced ways of communicating, accessing and receiving information that such technologies provide thus in exchange brings forth increased security issues and risks of personal data exploitation – this is also why internet and telecommunications technologies are constantly present in data protection debates.

[160] Mark Levene, *An Introduction to Search Engines and Web Navigation* (1st edn, Somerset Wiley (2011).
[161] EPIC, 'Search Engine Privacy' (2016) <https://epic.org/privacy/search-engine/> accessed April 4 2021; YourEurope, Data protection and online privacy (*EC*, 2021); Omer Tene, 'What Google Knows: Privacy and Internet Search Engines' [2008] 1433 WESTLAW 5-13.
[162] John Eustice, 'Understanding data privacy and cloud computing' (*Thomson Reuters*) <https://legal.thomsonreuters.com/en/insights/articles/understanding-data-privacy-and-cloud-computing> accessed April 4 2021.
[163] Microsoft Azure, 'What Is Cloud Computing? A Beginner's Guide' <https://azure.microsoft.com/en-us/overview/what-is-cloud-computing/> accessed April 6 2021.
[164] Gloria González Fuster, 'Big Data and Smart Devices and their Impact on Privacy' (EP, 2015) <https://www.researchgate.net/profile/Gloria-Gonzalez-Fuster/publication/289538954_Big_Data_and_Smart_Devices_and_their_Impact_on_Privacy/links/568ff7ce08aec14fa557b70b/Big-Data-and-Smart-Devices-and-their-Impact-on-Privacy.pdf> accessed April 14 2021, 12; .

### 3.2.2 SMART ELECTRONIC DEVICES

The use of internet and telecommunications technologies (e.g Cloud Computing, 5G, and WIFI) will be impossible without the help of smart electronic devices.[165] As *Fuster* explains, such devices refer to different forms of electronic equipment that are in principle controlled by individuals yet also have the ability to function interactively and autonomously.[166] Such devices further contain sensors and information-processing features enabling individuals to be informed, connected, productive and to provide different forms of entertainment.[167] Therefore, the development of smart electronic devices has become extensively attractive for users because it offers vast amounts of functionalities and abilities that accelerates our way of life.[168]

Devices such as computers and mobile phones are for instance smart electronics that are used for several purposes such as browsing the internet, writing documents, saving pictures and videos, watching movies, playing games etc. This substantially means that these are dependent on accepting, collecting, processing and storing the user's personal data to serve its purpose and improve thereof.[169] *Blanchette* therefore points out that such smart devices are often integrated with intrinsic features that are profoundly collecting different data that can include video and audio recording of a person's activities, work and physical and mental conditions such as body weight and sleep behaviours.[170]

These particular technologies therefore have limitless power and abilities to remember information of its users which ultimately reflects why we live in an era where most people are constantly recorded.[171] In comparison to other technologies, electronic devices have perhaps even more become an inevitable component in our lives,[172] yet users remain to lack understanding on how much of their data is being collected and how personal this information is, as well as experiencing difficulties for users to manage and

[165] Jake Frakenfield, 'Cloud Computing' (*Investopedia*, 2020) <https://www.investopedia.com/terms/c/cloud-computing.asp#:~:text=Key%20Takeaways-,Cloud%20computing%20is%20the%20delivery%20of%20different%20services%20through%20the,and%20retrieve%20them%20on%20demand> accessed April 11 2021; Deloitte, 'Data privacy in the cloud' <https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/risk/ca-en-risk-privacy-in-the-cloud-pov.PDF> accessed April 10 2021.

[166] Fuster (n 164).

[167] Praveena Devi and Others, 'A study on impact of electronic devices on youngsters' [2019] 8(5) The Pharma Innovation Journal 283-292; ICO, 'Smartphone security' <https://ico.org.uk/your-data-matters/online/smartphone-security/> accessed May 20 2021.

[168] Abdullahi Arabo and Others, 'Privacy in the Age of Mobility and Smart Devices in Smart Homes' [2012] IEEE 819.

[169] 'Computer', *Techopedia* <https://www.techopedia.com/definition/4607/computer> accessed April 4 2021; Lucas Introna, 'Privacy and the Computer: Why We Need Privacy in the Information Society' [1997] 28(3) Blackwell 259, 271-274.

[170] Yves Poullet and Others, *Computers, Privacy and Data Protection:An Element of Choice* (Springer 2011) 25.

[171] Ibid, 25-28.

[172] EDPS, 'Mobile devices' <https://edps.europa.eu/data-protection/data-protection/reference-library/mobile-devices_en> accessed April 17 2021.

restrict the data stored in their devices.[173] Therefore, smart electronic devices are considered as amongst world destruction weapons because as these offer increased connectivity these digital tools, these are also the reason behind the heightening privacy loss. [174]

### 3.2.3 SOFTWARES AND SYSTEMS

Today's electronic devices are to a great extent becoming smarter because these are additionally designed to operate and execute software and systems. A software is defined as an assembly of programmes and data instructing electronic devices on what to do, as well as how to accomplish the task given.[175] A system is on the other hand described as 'a network of related computer software, hardware, and data transmission devices' that can be used to conduct administrative or management work more efficiently.[176] These two concepts overlap to a degree because the term software relates to systems which are implemented using generic codes.[177] Nevertheless, it is important to differentiate these two concepts as systems sometimes involve much more sophisticated technologies that can manipulate the confidential or sensitive information obtained from data subjects.[178]

An application software is for instance known as the end user program that enables them to be productive in their every work. Some of these applications' software includes *Microsoft Word*, *Google Docs*, *Adobe Photoshop*, *Safari* etc. While systems such as *Windows*, *IOS* and *Android* which are considered as 'middlemen' tools between a user and the hardware (e.g. computer).[179] To cope up with development in digital tools, software and systems are constantly updated to preserve integration and functionality.[180] In comparison to tangible technologies such as smart devices, business today concentrates more on developing software or systems as it comes with lower

[173] Rani Molla, 'People say they care about privacy but they continue to buy devices that can spy on them' (*Vox*, 2019) <https://www.vox.com/recode/2019/5/13/18547235/trust-smart-devices-privacy-security> accessed April 17 2021.
[174] Ibid; Herb Weisbaum, 'Are the smart devices in your home spying on you?' (*BBT*, 2019) <https://www.nbcnews.com/better/lifestyle/downside-connected-tech-are-smart-devices-your-home-spying-you-ncna1101906> accessed April 16 2021; Nadine Guhr and Others, 'Privacy concerns in the smart home context' [2020] 2 SN Appl. Sci 247.
[175] 'Software' *Techopedia* <https://www.techopedia.com/definition/4356/software> accessed April 17 2021; FTMS, 'Computing Basics' [2019] CSCA0101 <https://ftms.edu.my/v2/wp-content/uploads/2019/02/csca0101_ch07.pdf> accessed April 18 2021, Chapter 7.
[176] Hillary G Sillitto, 'Defining "System"' [2017] 27 INCOSE https://www.researchgate.net/profile/Scott-Jackson-13/publication/318601827_Defining_System_a_Comprehensive_Approach/links/597282b3458515e26dfd9517/Defining-System-a-Comprehensive-Approach.pdf> accessed April 18 2021; Authenticity Consulting, 'What is a System?' LLC <https://managementhelp.org/systems/defn-system.pdf> accessed April 17 2021.
[177] John Spacey, 'Systems vs softwares' (*Simplicable*, 2016) <https://simplicable.com/new/systems-vs-software#:~:text=Technically%20speaking%2C%20a%20system%20is,term%20for%20any%20computer%20code> accessed March 29 2021.
[178] Ibid; Techopedia (n 175)
[179] Squareboat, 'Different Types of Software with Examples' <https://squareboat.com/blog/different-types-of-software-with-examples> accessed April 18 2021.
[180] Mourjo Sen and Others, 'Issues of Privacy and Security in the Role of Software in Smart Cities' [2013] ICCSNT.

distribution and variable costs and most importantly, it aligns with current market demands because these are key components in most digital technologies.[181]

Despite this, there is a lack of interest for developers to adopt good data protection practices and embedding privacy in their software or system developments.[182] An illustration of this is the video conferencing software called *Zoom* which have recently gained popularity amongst private individuals, organisations and even authorities. This software, however, quickly received security and privacy backlashes because the randomly generated ID that can be used to enter a conference call was found to be very 'easy to guess and even brute forceable'.[183] To that end, software and systems have become backbones of many digital technologies that sequentially threaten data protection because it captures big amounts of personal data and in many instances it lacks transparency on what information is collected and to whom these subjects are sharing their data with.

[181] Edward Muldrew, 'Why is there a demand for software product management?' (*Medium*, 2019) <https://edwardmuldrew.medium.com/why-is-there-such-a-demand-for-software-product-management-ffaf04da8731> accessed April 5 2021; Michael Marsiglia, '3 ways Software Products are Different from Physical Products' (*SAO*, 2014) <https://spin.atomicobject.com/2014/07/31/software-products-vs-physical products/#:~:text=Unlike%20physical%20products%2C%20software%20products,systems%20or%20web%20browsers%20updates> accessed April 5 2021.

[182] Awanthika Senarath and Nalin Arachchilage, 'Why developers cannot embed privacy into software systems?' [2018] EASE <https://arxiv.org/pdf/1805.09485.pdf> accessed April 5 2021, 1-6; Joachim Hackmann, 'How digitalization is changing the demand for software' (*Sitsi*, 2019) <https://www.sitsi.com/how-digitalization-changing-demand-software-development> accessed April 18 2021; Proctor Reid and Others, *Building a Better Delivery System: A New Engineering/Health Care Partnership* (NAP 2005) 63-82; HIPAA, 'Upgrading Software to comply with GDPR' (2018) <https://www.hipaajournal.com/upgrading-software-comply-gdpr/> accessed April 18 2021; Interact, 'Data management, privacy, and security in connected systems' [2018] Signify <https://www.interact-lighting.com/b-dam/b2b-li/en_AA/interact/articles/data-management/interact-sec-wp.pdf> accessed April 19 2021.

[183] Tom Warren, 'Zoom faces a privacy and security backlash as it surges in popularity' (*The Verg*e, 2020) <https://www.theverge.com/2020/4/1/21202584/zoom-security-privacy-issues-video-conferencing-software-coronavirus-demand-response> accessed April 18 2021.

# CHAPTER IV:
# THE CORONAVIRUS IMPACT

Digital technologies are not only the debated matter today as the Coronavirus outbreak, also known as COVID-19, are affecting all forms of companies, every social class, and are more particularly altering government's attention and priorities.[184] The WHO explained that the intensity of COVID-19 disease varies and depends on a person's health conditions but majority of those who get infected will experience respiratory illness and could create deadly damages in a person's body.[185] Even so, there was still a lot that was to be discovered about the COVID-19 because no one really had a clear picture of the level of threat this virus poses – ultimately leaving a degree of uncertainty on businesses and individuals on how to tackle and protect themselves from its dangers.

Yet as COVID-19 prolonged, the public demanded national authorities to unravel this disease, to provide information and strategy, and to provide reassurance that support, and assistance will be available for individuals and businesses during such a crisis.[186] Deciding on the most appropriate response to COVID-19 was hence difficult but comparing the measures that are being taken by different countries to see which has been the most successful and effective is an even more complicated task. [187]

Many national authorities therefore implemented a wide variety of measures to prevent and control the outbreak. Many Asian countries that are neighbours to China, where the crisis began, were for instance quick in responding and mitigating COVID-19 through aggressive lockdowns, self-isolation and closed borders. It was argued by *Tang* from Duke Global Health Institute that not all Asian countries followed the same response, but they found that

[184] Shahadat Uddin and Others, 'Onslaught of COVID-19: How Did Governments React and at What Point of the Crisis?' [2021] 24(1) PHM 1; Louise Miner and Others, 'How has the COVID-19 pandemic changed our lives globally?' (*EuroNews*, 2020) <https://www.euronews.com/2020/12/23/how-has-the-covid-19-pandemic-changed-our-lives-globally> accessed April 20 2021.
[185] Ibid (n 17).
[186] Chris Tyler and Peter Gluckman, 'Coronavirus: governments knew a pandemic was a threat – here's why they weren't better prepared' (The Conversation, 2020) <https://theconversation.com/coronavirus-governments-knew-a-pandemic-was-a-threat-heres-why-they-werent-better-prepared-136857> accessed April 17 2021; Uddin and Others (n 185); Amy Maxmen, 'Why did the world's pandemic warning system fail when COVID hit?' (*Nature*, 2021) <https://www.nature.com/articles/d41586-021-00162-4> accessed April 20 2021; Tim Paydos, 'The essential role of government during COVID-19' (*IBM*, 2020) <https://www.ibm.com/thought-leadership/institute-business-value/blog/covid-19-government> accessed April 21 2021.
[187] Oxford, 'COVID-19 Government Response Tracker' <https://www.bsg.ox.ac.uk/research/research-projects/covid-19-government-response-tracker> accessed April 22 2021; Roberto Rocha, 'What countries did right and wrong in responding to the pandemic' (*CBC*, 2020) <https://www.cbc.ca/news/canada/covid-19-coronavirus-pandemic-countries-response-1.5617898> accessed April 23 2021; Greenpeace, 'How the EU's response to the Covid-19 pandemic could make our society more resilient' *GEU*, 2020) <https://www.greenpeace.org/eu-unit/issues/democracy-europe/2673/how-the-eus-response-to-the-covid-19-pandemic-could-make-our-society-more-resilient/> accessed April 22 2021.

experiences that these countries have with previous pandemics played a significant role in their readiness to manage this crisis.[188]

On the other side of the globe, EU MS also had diverse measures in containing COVID-19 but careful considerations were further made on the action plans and restrictions to implement because these had to be weighed against impacts on citizen rights and societies well-being.[189] The EU thus fully activates the Integrated Political Crisis Response early 2020 after an immense increase of COVID cases happened in Italy.[190] As first on its agenda, the Union encouraged the assistance of MS on its COVID-19 response to not only protect people from COVID-19 but to support medical companies to guarantee its citizens access to safe and effective vaccines and to also accommodate socio-economic impact that accompanies this crisis.[191]

As restrictions on mobility and business operations were enforced, individuals were required to conduct work and education from their homes, along with organisations carrying out their daily businesses remotely to the extent possible.[192] Thus, the Coronavirus have left communities with no choice but to swiftly migrate to digital technologies for them to persevere and keep pace during this unprecedented time.

[188] ECDC, 'Data on country response measures to COVID-19' [2021] <https://www.ecdc.europa.eu/en/publications-data/download-data-response-measures-covid-19> accessed April 22 2021; Mely Caballero-Anthony, 'COVID-19 in Southeast Asia Regional pandemic preparedness matters' (*Brookings*, 2020)<https://www.brookings.edu/blog/order-from-chaos/2021/01/14/covid-19-in-southeast-asia-regional-pandemic-preparedness-matters/> accessed April 22 2021; Michel Penn, 'How Some Asian Countries Beat Back COVID-19' (*DGHI*, 2020) <https://globalhealth.duke.edu/news/how-some-asian-countries-beat-back-covid-19> accessed April 23 2021; Naomi Xu Elegant, 'How countries in Asia kept a handle on COVID-19 outbreaks' (*Fortune*, 2020) <https://fortune.com/2020/12/28/asia-covid-success-stories-lessons-learned/> accessed May 1 2021.

[189] ECHR (n 4) Article 15; FRA, 'Coronavirus Pandemic in the EU Fundamental Rights: Focus on Social Rights Implications' (2020) 6 <https://fra.europa.eu/sites/default/files/fra_uploads/fra-2020-coronavirus-pandemic-eu-bulletin-november_en.pdf> accessed March 18 2021, 15-19; EPRS, 'Upholding human rights in Europe during the pandemic' (2020) <https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/652085/EPRS_BRI(2020)652085_EN.pdf> accessed March 18 2021.

[190] EC, 'Timeline COVID-19 coronavirus' (*EU*, 2021) <https://www.consilium.europa.eu/en/policies/coronavirus/timeline/> accessed May 1 2021, see e.g. timeline from February to March; EC, 'How the IPCR crisis response mechanism works' (*EU*, 2020) <https://www.consilium.europa.eu/en/infographics/ipcr-mechanism/#:~:text=Text%20version,complex%20crisis%2C%20including%20terrorist%20acts> accessed April 22 2021.

[191] BBC, 'Covid: How are European countries tackling the pandemic?' (2020) <https://www.bbc.com/news/explainers-53640249> accessed April 30 2021; Claire Busse and Others, 'The crisis that made the European Union: European cohesion in the age of covid' (ECFR, 2020) <https://ecfr.eu/publication/the-crisis-that-made-the-european-union-european-cohesion-in-the-age-of-covid/> accessed May 1 2021.

[192] Stefana Miladinovic, 'Is COVID-19 accelerating digitalisation or exposing the digital divide?' (*NewEurope*, 2020) <https://www.neweurope.eu/article/is-covid-19-accelerating-digitalisation-or-exposing-the-digital-divide/> accessed May 2 2021; Aamer Baig and Others, 'The COVID-19 recovery will be digital: A plan for the first 90 days' [2020] McKinseyDigital 1.

## *4.1 THE ACCELERATION OF DIGITALIZATION*

The ongoing COVID-19 crisis has necessitated people to find creative ways of performing work, education, business and other daily activities. For that reason, digital technologies serve as the key to not only proceed with our daily tasks and businesses or to stay connected but to also remain informed about the present state of virus spread.[193] According to a survey by *Mckinsey*, [194] COVID-19 presented the benefits of digital technologies because they have been a key help in gathering information, facilitating services and controlling the spread of infections through tracing – this in turn has accelerated societies and companies' digital use by around three to ten years.[195]

An example of this is the digital tool launched by *Oxford University* for online tracking governments COVID-19 responses all over the world. This tool aims to e.g., provide hard evidence on the effectiveness of different measures to guide regulators in their response's assessments.[196] Similarly, a mobile application called ZOE was launched by a British health science company in the beginning of the crisis when virus testing was limited. [197] This application encourages individuals to report all COVID-19 symptoms they are experiencing. By doing so, the Company is able to study and understand this disease better, as well as to offer valuable information to governments on how infectious this virus is and how quickly these are transmitted.[198]

As the Coronavirus crisis and accelerated digitalization simultaneously occur, some researchers believe that these events have revealed underlying societal issues such as uneven access to digital tools, privacy intrusions and warrantless surveillance.[199] Thus, current EU DPR and digital agendas are being worked on and reflected upon by the EC in order to complement measures being taken to deal with this pandemic, as well as to existing defeat threats such as on data protection.[200]

[193] O A Nesterchuk and Others, 'Digitalization as the "new normal" of higher education' [2020] 1691(1) Journal of physics 12068; Peter Dannenberg and Others, 'Digital Transition by COVID-19 Pandemic?' [2020] 111(3) TESG 543-560.
[194] Laberge and Others (n 16); Samer Faraj and Others, 'Unto the breach: What the COVID-19 pandemic exposes about digitalization' [2021] 31(1) McGill University 100337, 2-5.
[195] Faraj and Others (n 194); United Nations, 'Digital technologies critical in facing COVID-19 pandemic' (DESA, 2020) <https://www.un.org/fr/desa/digital-technologies-critical-facing-covid-19-pandemic> accessed May 9 2021; Ibid (n 19).
[196] Ibid (n 193): Rocha (n 187).
[197] ZOE, 'COVID Symptom Study' <https://covid.joinzoe.com/about> accessed May 4 2021.
[198] Lund University, 'COVID Symptom Tracker app launched in Sweden' (*LU*, 2020) <https://www.lunduniversity.lu.se/article/covid-symptom-tracker-app-launched-sweden> accessed May 5 2021.
[199] Faraj and Others (n 194).
[200] EC, 'Shaping Europe's digital future: Digital Single Market' <https://ec.europa.eu/digital-single-market/en> accessed May 9 2021.

## *4.2 THE GDPR AND GLOBAL PANDEMIC RESPONSE*

Around the same time that COVID-19 first affected Europe, the EC had just released a report on the first two years of the GDPR which demonstrated that the Regulation is successfully meeting its objective, especially in providing citizens strong sets of enforceable rights and in equipping DPA with stronger corrective powers to implement these rules.[201] While this is a positive outcome, researchers have found that there remains a great number of online privacy policies within the EU that are not fully compliant. On top of that, the pandemic has shifted lawmakers' priorities and has been stalling agendas concerning data protection policies within the EU.[202]

These global responses to COVID-19 are undoubtedly urgent and should be the main focus of authorities right now which is why companies, governments and researchers are working together to develop solutions (e.g. tests, treatments and vaccines) and to make use of digital technologies in this process.[203] However, this has further led these actors to question whether the GDPR will be an obstacle in its response to COVID-19, to what extent can a citizens' right to privacy be lawfully restricted and under what conditions.[204] Likewise, DPR has been fronted with a drastic amount of data breaches since the start of COVID-19 because some companies use the current event as an opportunity to get hold of sensitive data and abuse for their own advantage.[205]

The ICO shares the opinion that COVID-19 is presenting intensified threats on digital rights and right to information because despite the pandemic accelerating digital technologies, these manage some of the most personal and sensitive data of individuals (i.e. patients, employees, students, customers and

[201] EC, Empower citizens for digital age (n 7); FRA, 'Your rights matter: data protection and privacy' [2020] EU <https://fra.europa.eu/sites/default/files/fra_uploads/fra-2020-fundamental-rights-survey-data-protection-privacy_en.pdf> accessed May 2 2021; Livia Puljak and Others, 'Before and after enforcement of GDPR' [2020] 30(3) BiochemMed 030201; Sean Illing and Marisa Brookes, 'The European Commission reports after two years of the GDPR' (*Lewis Silkin*, 2020) <https://www.lewissilkin.com/en/insights/the-european-commission-reports-after-two-years-of-the-gdpr> accessed May 2 2021.

[202] Illing and Brookes (n 201); Razieh Zaeem and Others, 'The Effect of the GDPR on Privacy Policies: Recent Progress and Future' [2020] 12(1) ACM 14-18; Thomas Linden and Others, 'The privacy policy landscape after the GDPR' [2019] Scienda 1-18; Steven Murdoch and Apa Kapadia, 'PoPETs' [2020] 4 Sciendo, 47–64.

[203] Regina Becker, 'COVID-19 Research: Navigating the European General Data Protection Regulation' [2020] 22(8) JMIR E19799.

[204] Magdalena Kedzior, 'The right to data protection and the COVID-19 pandemic: the European approach' [2020] 21 ERA 533-543; Hogan Lovells, 'Coronavirus and data protection – Guidance by data protection authorities' [2020] <https://www.hoganlovells.com/~/media/hogan-lovells/pdf/2020%20PDFs/2020_03_19_Coronavirus_and_data_protection_Guidance_by_DPAs.pdf> accessed May 3 2021; Ventrella (n 21) 2.

[205] Empower citizens for digital age (n 7); FRA, Your rights matter: data protection and privacy (n 201); Puljak and Others (n 201); Costica Dumbrava, 'Lifting Coronavirus Restrictions' [2020] EPRS 652.016 <https://op.europa.eu/en/publication-detail/-/publication/24f80771-d143-11ea-adf7-01aa75ed71a1/language-en> accessed May 7 2021. Daniel Lohrmann, '2020: The Year the COVID-19 Crisis Brought a Cyber Pandemic' (GovTech, 2020) <https://www.govtech.com/blogs/lohrmann-on-cybersecurity/2020-the-year-the-covid-19-crisis-brought-a-cyber-pandemic.html#:~:text=One%20specific%20example%20comes%20from,cyberattacks%20in%20late%20April%202020.&text=%22Since%20the%20start%20of%20the,targeting%20the%20public%20at%20large> accessed May 3 2021.

web users).[206] The use of digital tracing tools to mention personal information such as names, address, recent locations and activities) of those who have been in contact with an infected patient is an illustration of this.[207] Such contact tracing is done with the help of electronic devices or software which help track infected patients and their recent contacts through GDPS locations or Bluetooth signalling.[208]

Although many companies will reassure that these data are secured, the entities rely on anonymisation such as use unique numeric identifiers which any cyberintruder with adequate technical skills can effortlessly link this to the particular device and data subject.[209] An example of this is Apple-Google's contact tracing application that collects location data of millions of users in countries such as Switzerland, USA, Australia and South Korea. This Application has said to have helped control the infection spread, however, governments using these have not concretely demonstrated the App's privacy standards and compliance.[210]

Moreover, a number of these apps are built to process the user's data even before a data subject has given its consent and the moment it is downloaded, as well these data transfers to systems that may be accessible to different entities and actors.[211] Therefore, it is not only the effectiveness of these digital contact tracing that policy makers should be concerned of but also how to address the privacy challenges arising from these digital tracing tools. [212]

According to *Bradford*, the demand on digitally tracking people's locations and health status as much as possible presents a vital stress or enforcement

[206] Stephens Harwood, 'Data protection and coronavirus: what you need to know' (2020) <https://www.shlegal.com/news/data-protection-and-coronavirus-what-you-need-to-know> accessed May 3 2021; ICO, 'Updated regulatory approach in response to the coronavirus pandemic' [2020] 3(1) ICO.

[207] EpiServer, 'COVID-19's impact on data privacy, protection and security' <https://www.episerver.com/guides/covid-19-privacy-considerations> accessed May 7 2021.

[208] CDC, 'Contact Tracing: Using Digital Tools and Monitoring the Disease' (2019) <https://www.cdc.gov/coronavirus/2019-ncov/cases-updates/about-epidemiology/monitoring-and-tracking.htm> accessed May 7 2021; WHO, 'Digital tools for COVID-19 contact tracing' [2020] <https://apps.who.int/iris/rest/bitstreams/1279465/retrieve> accessed May 7 2021.

[209] Laura Bradford, 'COVID-19 contact tracing apps: a stress test for privacy, the GDPR, and data protection regimes' [2020] 7(1) JLB 3-5; Kirsten Bock and Others, 'Data Protection Impact Assessment for the Corona App' [2021] 1(6) FIfF 46 <https://www.researchgate.net/publication/348618489_Data_Protection_Impact_Assessment_for_the_Corona_App/fulltext/6007a065a6fdccdcb868a2f6/Data-Protection-Impact-Assessment-for-the-Corona-App.pdf> accessed April 29 2020; Stuart Thompson and Charlier Warzel, 'Smartphones are Spies. Here's Whom They Report to' (*New York Times*, 2019) <https://www.nytimes.com/interactive/2019/12/20/opinion/location-tracking-smartphone-marketing.html> accessed May 4 2021.

[210] NYT, 'Google Coronavirus Apps Give it Way to Access Location Data' (*New York Times*, 2020) <https://www.nytimes.com/2020/07/20/technology/google-covid-tracker-app.html> accessed May 4 2021; Steven Overly and Mohan Ravindranath, 'Google and Apple's rules for virus tracking apps sow division among states' (*Politico*, 2020) <https://www.politico.com/news/2020/06/10/google-and-apples-rules-for-virus-tracking-apps-sow-division-among-states-312199> accessed May 8 2021; Bock and Others (n 209).

[211]Tamar Sharon, 'Blind-sided by privacy? Digital contact tracing, the Apple/Google API and big tech's newfound role as global health policy makers' [2020] EIT 1-3; Bock and Others (n 209); Giuseppe Persiano, 'Joint Statement on Contact Tracing represented by scientists and researchers from across the globe' [2019] <https://giuper.github.io/JointStatement.pdf> accessed May 8 2021.

[212] Ibid; Federica Lucivero and Others, 'COVID-19 and Contact Tracing Apps: Technological Fix or Social Experiment?' [2020] 1 SSRN.

test to EU's and other international nascent privacy regimes (such as the GDPR and Organisation for Economic Cooperation and Development's (hereinafter 'OECD') Privacy Guidelines).[213] This means that as COVID-19 accelerates digitalization, it also unfolds current EU DPR' flexibility and capability to answer new and compound data protection issues.

Some employers are for instance using electronic devices that are incorporated with tracking and communicating solutions to record employees' locations and better identify risk of infections.[214] Some of this information may then be shared with authorities and other entities. [215] For students, however, the spread of infection is e.g. controlled by institutions through use of surveillance cameras that measure students' body temperature.[216] The use of such tools are perhaps based on good intentions of protecting the public and the processing of such may be covered by the GDPR and other national privacy regimes (such as FERPA,[217] HIPAA[218], DPA,[219] CPRA,[220] and PAIS[221]) for companies and institutions are additionally fronted with the difficult choice of either gathering as much personal information to contain the virus spread or protect these individual privacy rights.

Nevertheless, the current situation gives them an ability to restrict data protection rights by simply using COVID-19 as a justification for obligating employees and students to disclose and process personal information that are

[213] Bradford (n 209) 3-4 and 7-10.

[214] TrustArc, 'Managing Employee Privacy in the Face of COVID-19' (*TrustArc*, 2020)<https://trustarc.com/blog/2020/03/19/managing-employee-privacy-in-the-face-of-covid-19/> accessed April 27 2021; A4L, 'Student Privacy and COVID-19' [2020] <https://cdn.ymaws.com/www.a4l.org/resource/resmgr/docs/whitepaper/student_privacy_and_covid-19.pdf> accessed April 21 2021.

[215] Jason Beaubin, 'More Companies Are Using Technology To Monitor For Coronavirus In The Workplace' (*NPR*, 2020) <https://www.npr.org/2020/10/13/918315238/more-companies-are-using-technology-to-monitor-for-coronavirus-in-the-workplace?t=1619293477836> accessed April 27 2021; Aiha Nguyen, 'On the Clock and at Home: Post-COVID-19 Employee Monitoring in the Workplace' (*SHRM*, 2020) <https://www.shrm.org/executive/resources/people-strategy-journal/summer2020/Pages/feature-nguyen.aspx> accessed April 28 2021

[216] Colin Lecher, 'Schools Are Buying Up Surveillance Technology to Fight COVID-19' (*MarkUp*, 2018) <https://themarkup.org/coronavirus/2020/09/08/school-reopening-surveillance-contact-tracing> accessed May 3 2021; Drew Harwell, 'Mass school closures in the wake of the coronavirus are driving a new wave of student surveillance' (*TWP*, 2020) <https://www.researchgate.net/publication/347933515_Need_for_faster_response_of_education_and_research_system_to_covid_-19_English_version> accessed May 8 2021.

[217] USA Family Educational Rights and Privacy Act (FERPA) of 1974.

[218] USA Health Insurance Portability and Accountability Act (HIPAA) of 1996; OCR, 'Summary of the HIPAA Privacy Rule' [2020] <https://www.hhs.gov/sites/default/files/privacysummary.pdf> accessed May 5 2021.

[219] LTP, 'A Regional Guide to Employee Data Privacy' [2018] <https://www.leetsai.com/wp-content/uploads/2018/12/Regional-Guide-to-Employee-Data-Privacy-Asia-2018-LTP.pdf> accessed May 5 2021, 87-93; see also Singapore's PDA 94-103.

[220] IApp, 'The California Privacy Rights Act of 2020' [2020] <https://iapp.org/resources/article/the-california-privacy-rights-act-of-2020/> accessed May 5 2021.

[221] EC, 'Digital solutions during the pandemic' <https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/digital-solutions-during-pandemic_en> accessed May 3 2021; Marko Teräs and Others, 'Post-Covid-19 Education and Education Technology 'Solutionism': a Seller's Market' [2020] 2 PSE 863, 385-387; Neil Selwyn, 'What's the problem with learning analytics?' [2020] 6(3) JLA, 11– 19.

otherwise not known to them.[222] Although it is apparent that public health safety outweighs privacy in this context, advocates shed light on data breaches that are also expanding in macro scales as governments and big companies join forces to put an end to the virus.[223] From the data subjects perspective, divulging their sensitive life details greatly impacts them because not all businesses or governments may use their data for other purposes other than public health safety.

Hence *Boudreaux and Fukuyuma* believes that 'privacy violations will [have] significant social implications for both the public's trust and [authorities' accountability,] in general and in the specific context of [organisations, institutions and] government's response to the COVID-19 crisis'.[224] In order to maintain data privacy enforcement balanced with the pandemic response, regulators thus need to set up clear and legal guidelines in government and businesses use of digital technologies as a tool against COVID-19.[225]

[222] Ibid (n 119): TrustArc (n 214); Anisha Reddy and Amelia Vance, 'Student Privacy during the Pandemic' [2020] AASA <https://iapp.org/media/pdf/resource_center/fpf_student_privacy_during_covid_19_pandemic.pdf> accessed May 3 2021, 2-9; CWB, 'Balancing Employee Privacy and Protection' <https://www.corporatewellnessmagazine.com/article/covid-19-balancing-employee-privacy-and-protection> accessed May 8 2021; A4L (n 214) 1-3; Baker Mckenzie, 'COVID-19 Privacy and Security Survey' [2019] <https://www.bakermckenzie.com/-/media/files/insight/publications/2020/04/covid19-data-privacy--security-survey17-april.pdf> accessed April 30 2021.

[223] Teräs and Others (n 221); PWC, 'Balancing employee privacy and public health and safety' <https://www.pwc.com/us/en/library/covid-19/global-privacy-impact-assessment.html> accessed May 8 2021; Persiano (n 212).

[224] Benjamin Boudreaux and Others, 'Data Privacy During Pandemics: A Scorecard Approach for Evaluating the Privacy Implications of COVID-19 Mobile Phone Surveillance' [20202] RAND 2-6, and 30; Francis Fukuyama, 'The Thing That Determines a Country's Resistance to the Coronavirus' (*Atlantic*, 2020) <https://www.theatlantic.com/ideas/archive/2020/03/thing-determines-how-well-countries-respond-coronavirus/609025/> accessed May 5 2021; Hannah van Kolfschooten and Anniek de Ruijter, 'A legal perspective on contact tracing' [20202] 41(3) CSP 478-491.

[225] ICO, What you need to know (n 23); ICO, Updated regulatory approach (n 206); Bradford (n 209) 3-5.

# CHAPTER V:
# TO PROTECT LIVES AND DATA PRIVACY

The Coronavirus has indeed brought along ambiguities in our daily lives and how it will impact our collective future, but it certainly exhibited how useful digital technologies are in overcoming such a crisis.[226] Yet as companies and governments are faced with such unprecedented challenges and issues relating to privacy, regulators' role have become even more crucial in ensuring data protection will not be compromised in times of distress. Hence as *Ventrella* points out:

> When the impact of COVID-19 on privacy and the protection of personal data first started to become visible, privacy experts in Europe denounced the unavoidable "Big Brother" coming out of the privacy vs. health trade-off. These fears did not overestimate the potential impact of this catastrophic event. They did however underestimate the power and effectiveness of the European data protection regime.[227]

Since Coronavirus is a shared crisis that all nations are working fast to conquer, the EU expressed that current DPR should therefore not be seen as opposing measures taken against this infectious disease.[228] In fact, Article 9 GDPR identifies health data as a special category that is in principle prohibited under this provision unless it pursues one of the listed conditions such as reasons of public interest or where personal data processing is necessary for protection of public health such as the COVID-19.[229]

Moreover, this provision follows similar rules as any processing of personal data and as legal scholars point out that while MS are given the discretion to implement efforts against COVID-19, it is not sufficient to move along with processing because Article 9 contains strict requirements and conditions that need to be fulfilled. [230] Be that as it may, the EDPB stresses in Guidelines 03/2020 that it vital for organisations to fully understand who, what and when a processing operation can benefit from a special regime that is foreseen in Article 9 before relying on this provision.[231]

---

[226] Jeffrey L. Turner, 'Privacy and Security in the Post-Pandemic World' [2021] 11(115) NLR <https://www.natlawreview.com/article/privacy-vs-security-post-pandemic-world> accessed May 1 2021.
[227] Ventrella (n 21) 392; Lambert (n 24).
[228] EDPS, Statement on the processing of personal data (n 24).
[229] GDPR (n 7) Article 9; Santa Slokenberga and Others, *GDPR and Biobanking* (1st edn, Springer 2021) 23-27.
[230] Ibid; Reichel Lind, 'The new general data protection regulation—where are we are and where might we be heading?' [2015] 14 Springer 95-100; Deborah Mascalzoni, 'Ethics, law and governance of biobanking' [2015] 14(1) Springer 53-77.
[231] EDPB, Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak (adopted 21 April 2020) 4-7.

More so, it signifies that still have to secure that its purpose for are based on one of the lawful grounds provided by Article 6 GDPR (e.g section *(c)* or *(d))* and to demonstrate the appropriateness of such basis to its processing activities, as well as it respects principles set out in Article 5 GDPR that maintains the obligations of controller and processor towards users' personal data security.[232] In the context of digital tracking and other surveillance technologies whose objective is to detect early signs of symptoms, tracing and monitoring individuals are therefore required to carefully evaluate why such data are collected and how it is managed.[233]

The fact that Article 9 GDPR categorises health data as sensitive, it exhibits the dangerous consequences that it may create on individuals' data integrity if such are exposed to malicious attacks.[234] Yet the A29WP construes that health data is a broad concept associated to 'clearly medical data, raw sensor data that can be used in itself, or in combination with other data to draw conclusion about the actual health status or health risk of a person, or conclusions are drawn about a person's health status or health risk'.[235] It therefore necessitates that processing of these forms of personal data should only be granted when explicit consent from data subjects or employees has been obtained.[236]

In the context of employment relationships and the current privacy issues arising from COVID-19, it is difficult to determine whether consent has been indeed freely given because employees may feel the need to agree to disclose information or to track to avoid facing potential consequences from such refusal.[237] Companies, whether a controller or process, that decide to put health monitoring schemes in workplaces must thus refrain from taking advantage of their authority and indirectly coercing personal data from individuals. Instead, it should pursue transparency towards its employees by

[232] Ibid 8-13; Giulia Schneider, 'Disentangling health data networks' [2019] 9(4) IDPL 267–271; Celine Olsen, 'To track or not to track? Employees' data privacy in the age of corporate wellness, mobile health, and GDPR' [2020] 10(3) IDPL 236-252; Luca Marelli and Others, 'Fit for purpose? The GDPR and the governance of European digital health' [2020] 41(5) Policy Studies 447, 479.

[233] David Cox, 'The rise of employee health tracking' (*BBC*, 2020) <https://www.bbc.com/worklife/article/20201110-the-rise-of-employee-health-tracking> accessed April 28 2021; Olsen (n 232) 243.

[234] GDPR (n 7) Recital 35; Olsen (n 232) 243–245.

[235] A29WP Letter to clarify the scope of the definition of data concerning health (5 February 2015) <https://ec.europa.eu/justice/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_en.pdf> accessed April 28 2021, 1–2; Olsen (n 232) 244.

[236] Ibid; Sandra Wachter and Brent Mittelstadt, 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI' [2019] 2(1) CBLR 461 para 9.

[237] GDPR (n 7) Article 4 (11); Olsen (n 232) 243 - 245; Robert Lister, Employee monitoring during the COVID 19 lockdown GDPR considerations revisited' [2020] R&G <https://www.ropesgray.com/-/media/Files/alerts/2020/05/20200504_COVID_London_Alert.pdf> accessed May 1 2021, 1-4; Guidelines 05/2020 on consent

providing them with adequate processing information, the power to decide and control which personal data they are prepared to share.[238]

To consider EU DPR as an impediment on the use of digital technologies as a tool against COVID-19 is to some extent exaggerated because it is demonstrating to preserve data protections standards and data integrity of individuals, at the same time to guide entities in its pandemic responses. As expressed in the *Two Years Plan of the eHealth Network Meetings and Sustainability*, digital health technologies and the data it collects has on many occasions drawn EU regulators attention which is precisely the reason why Directive 2011/ 24/EU[239] was laid out.

The objective of this Directive is to govern cross-border exchange of health data within the EU, as well as to call attention to its obligations under the former Data Protection Directive, now the GDPR.[240] Such a legal framework is thus supplementing protection of health data processing, especially today where such data are not only processed by European establishments but may be further shared with entities beyond its perimeters as many of the health companies developing vaccines and other preventive solutions against COVID-19 are situated in a third country.[241]

With regards to digital solutions used in the COVID-19 fight that instead gathers other sensitive data, privacy regulators reassures that current DPR are adequately flexible to govern these and address the issues it raises.[242] This can however not be simply translated as guaranteeing that privacy challenges are temporary and can easily be overcome because digital technologies develops on high-speed,[243] sequentially implying that European and local authorities need to continuously guide organisations and governments in balancing protection of lives with data privacy.[244] The *Nuffield Council on Bioethics* adds that whilst the COVID-19 battle may be the best reason for

[238] Lister (n 237); Kedzior (n 204) 534-537; ILO, 'An employers' guide on working from home in response to the outbreak of COVID-19' [2020] < https://www.ilo.org/wcmsp5/groups/public/---ed_dialogue/---act_emp/documents/publication/wcms_745024.pdf> accessed May 1 2021 14-16; UNISON, 'Monitoring and surveillance workplace policies' [2020] <https://www.unison.org.uk/content/uploads/2020/07/Monitoring-and-surveillance-at-work-1.pdf> accessed May 2 2021.

[239] Council Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare [2011] OJ L 88 Preamble section 25; EC, 'Two years plan of the eHealth Network meetings and sustainability' [2019] V1.3 <https://ec.europa.eu/health/sites/health/files/ehealth/docs/ev_20190611_co512_en.pdf> accessed May 2 2021; EC, 'Exchange of electronic health records across the EU' <https://digital-strategy.ec.europa.eu/en/policies/electronic-health-records> accessed May 2 2021.

[240] Ibid (n 2).

[241] Ibid.

[242] Mathew Schwartz, 'Privacy Regulator Promises 'Flexibility'' (*BIS*, 2020) <https://www.bankinfosecurity.com/gdpr-covid-19-privacy-regulator-promises-flexibility-a-14177> accessed May 2 2021; EDPS, Statement on the processing of personal data (n 24); Carmel Shachar and Others, 'AI Surveillance during Pandemics: Ethical Implementation Imperatives' [2020] THC 50(3) 18-21.

[243] EDPS, Statement on the processing of personal data (n 24).

[244] EDPB, Guidelines 03/2020 (n 234).

collecting sensitive data without consent, organisations have to be reminded that such activities requires to be ethically justified and of strict necessity to avert harm from the public – and even so, data subjects' power over their data should be utmost preserved especially in such a time.[245]

## *5.1 A FAIR BALANCE BETWEEN DATA RIGHTS AND PUBLIC HEALTH*

It was mentioned earlier that several EU legislations and instruments allow for rights and freedoms to be restricted in times of emergencies through a form of special regime or exemption clause. However, this generally does not render the law inapplicable or suspended because its objective is to permit restrictions only in absolute necessity and within a defined duration so that citizens remain protected in times of distress.[246] This kind of rule is evident in Article 89 (3) GDPR ensures that protection of personal data is not undermined even when processing is conducted for public interest or general health purposes. This provision states that:

> Where personal data are processed for archiving purposes in the public interest, [EU MS] may provide for derogations from the rights referred to in Articles [15 to 21] subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.[247]

On the top of that, Article 89 (1) reiterates controllers and processors to implement adequate security, technical and operational measures (such as data minimisation and pseudonymisation) to the best of its ability, and to reflect upon whether the manner that these digital tools are used to support efforts against the Coronavirus crisis safeguards the protection of personal data enshrined in the GDPR. This also includes evaluating whether

[245] NCB, 'Guide to the Ethics of Surveillance and Quarantine for Novel Coronavirus' <https://www.nuffieldbioethics.org/assets/pdfs/Guide-to-the-ethics-of-surveillance-and-quarantine-for-novel-coronavirus.pdf> accessed May 4 2021; Shachar and Others (n 242); DGHS, 'Assessment of the EU Member States' rules on health data in the light of GDPR' <https://ec.europa.eu/health/sites/health/files/ehealth/docs/ms_rules_health-data_en.pdf> [2021] accessed May 5 2021, 50-56; Dyani Lewis, 'Contact-tracing apps help reduce COVID infections, data suggest' (*Nature*, 2021) <https://www-nature-com.db.ub.oru.se/articles/d41586-021-00451-y> accessed May 4 2021.

[246] COE, 'COVID-19 and Data Protection' <https://www.coe.int/en/web/data-protection/covid-19-data-protection> accessed May 5 2021.

[247] GDPR (n 7) Article 89 (1).

processing in the context of COVID-19 satisfies the 'necessity criteria' under Article 89.[248]

In such a case, Article 52 (1) of EU Charter also emphasizes that such restriction on privacy rights should not go farther than what is demanded and to the extent that its detriments to those rights. Hence, any processing activities must consider the degree of sensitivity of such data in question and because these levels of sensitivity differ in MS, the GDPR have identified a list of sensitive data such as those referred in Article 9 and in the EC's decision on the adequacy of protection provided by the Safe Harbor.[249]

It can therefore be claimed that the situation, such as COVID-19 and accelerated digitalization, that demands big tech companies to collaborate with health researchers and provide value to their studies through sharing massive amounts of personal health data may have been anticipated by EU legislators when drafting the GDPR.[250] This is because even if Article 9 and 89 GDPR permits restrictions on right to data protection for public health purposes, the Regulation attempts to set boundaries on such cases through explicitly setting up conditions and safeguards.[251]

Hence, the EC refers to Article 3 of the Regulation (EC) No 1338/2008 on public health and health and safety at work where it defines public health as all elements or factors relating to health such as health status, diseases and health care.[252] This broad definition affirms that the use of digital solutions in the COVID-19 fight may perhaps conform to these exemption clauses because these serve the interest of the public and their health.[253] It is evident that the scope of these clauses are still relatively unclear and may legitimate a number of processing activities during this crisis that ultimately yield large corporations to misuse and hide under the 'protection of public health' facade.[254]

Therefore, necessary processing of medical data for vaccines and other preventive medicines should be closely governed by an agreement between parties ensuring security measures are followed, explicit tasks are delegated,

[248] GDPR (n 7) Recital 157, Articles 6(4) and 5(1); European Parliamentary Research Service (EPRS), 'How the General Data Protection Regulation changes the rules for scientific research' [2019] PE 634.447; EDPS, Opinion 20 November 2017 10/2017, on safeguards and derogations under Article 89 GDPR in the context of a proposal for a Regulation, 7; A29WP, Opinion of the European Data Protection Supervisor on the data protection reform package [2012] C 192/7.
[249] Ibid (n 133); Danny Koevoets, 'The Influence of Article 89 GDPR on the Use of Big Data Analytics for the Purpose of Scientific Research' [2015] TU <http://arno.uvt.nl/show.cgi?fid=142885> accessed May 6 2021, 16-20; GDPR (n 7) Article 83(1)(b); A29WP Advice paper on special categories of data ("sensitive data") [2012] ARES 444105.
[250] Schneider (n 232).
[251] GDPR (n 7) Recital 157; Schneider (n 232) 165-268.
[252] Ibid, Recital 54; Regulation (EC) 1338/2008 of the European Parliament and of the Council of 16 December 2008 on Community statistics on public health and health and safety at work (Public Health Statistics) OJ L 354/70.
[253] Schneider (n 232) 268.
[254] Ibid; Slokenberga and Others (n 230).

as well as making sure that data are solely processed within said purpose just as prescribed by the GDPR.[255] Since Article 15 of the EPD[256] allows EU MS to adopt emergency legislations to e.g. protect the public from health threats, processors and controllers must consider present Coronavirus frameworks that aim to guide them in their action plans and use of digital tools to curb down COVID-19 cases. [257]

The EU DPR and recent frameworks on data protection promote fair balancing of efforts against the pandemic with citizens' rights and freedom, setting out limitations on the use of exemption and derogatory provisions in emergencies, and promoting accountability in the use of digital technologies during such a time.[258] According to a joint statement by *Pierucci* and *Walter,* these frameworks maintain high standards for the protection of personal data which are compatible and reconcilable with other fundamental rights and relevant public interests. [259]

To this end, it conveys that privacy regimes are not in any way hindering the use of digital technologies mitigating the infection spread because as the EDPB underlines:

> One should not have to choose between an efficient response to the current crisis and the protection of our fundamental rights: we can achieve both, and moreover data protection principles can play a very important role in the fight against the virus. European [DPR rather guarantees] the responsible use of personal data for health management purposes, while also ensuring that individual rights and freedoms are not eroded in the process.[260]

The GDPR nevertheless remains steadfast amidst COVID-19 and accelerated digitalization, as it drives fair balancing of these two interests.[261] Yet as argued by scholars, fundamental rights such as data rights are not absolute signifying that other rights and public security may outrank this.[262] Even so,

---

[255] Stuart McLennan, 'COVID-19: Putting the General Data Protection Regulation to the Test' [2020] 6(2) JMIR E19279; Jo Joyce, 'Sharing personal data in the context of COVID-19' (*GDH*, 2020) <https://globaldatahub.taylorwessing.com/article/sharing-personal-data-in-the-context-of-covid-19> accessed May 6 2021.
[256] EPD (n 118) Article 15.
[257] COE, 'Statement by Alessandra Pierucci and Jean-Philippe Walter' (2020) <https://www.coe.int/en/web/data-protection/statement-by-alessandra-pierucci-and-jean-philippe-walter> accessed May 6 2021; McLennan (n 255); Katharine Wallis and Others, 'Research using electronic health records: Balancing confidentiality and public good' [2018] 10(4) JPHC 288; The Lancet Respiratory Medicine, 'Data protection: balancing personal privacy and public health' [2015] 4(1) LRM 1.
[258] See for example: EC, Communication from the Commission Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection (2020) OJ C 124I; UK's Coronavirus Act 2020 Chapter 7; EDPB, Guidelines 03/2020 (n 234).
[259] COE (n 57) Statement; Shachar and Others (n 242).
[260] Shindler (n 23).
[261] GDPR (n 7) Articles 5 (1 b and e), Article 14 (5b) and Article 17 (3d); EDPB, Guidelines 03/2020 (n 234).
[262] EU Charter (n 5) Article 52(1 and 2); Michele Finck and Frank Pallas, 'They who must not be identified—distinguishing personal from non-personal data under the GDPR' [2015] 10(1) IDPL 34; Shachar and Others (n 242) 21

processors and controllers should remain transparent, aim for diligence, data minimisation and storage limitation,[263] as well as to respect existing legal frameworks because the race to save lives is composed of the goal to protect individuals' health and overall well-being.[264]

## *5.2 MOVING FORWARD WITH PRIVACY, DIGITIZATION AND COVID-19*

It is safe to say that restricting data rights in the context of COVID-19 is permitted but it is also worth pointing out that such have to be assessed on a case-to-case basis. The GDPR additionally emphasizes that whilst its primary and most important goal is to empower data protection, it also pursues strengthening the internal market and its economies.[265] Digital technologies are thus not only valuable in the COVID-19 fight as DSM also aims to utilize these to develop societies and economies within the Union.[266] Yet to succeed in advancing European communities through digital technologies, the EU highlights the need to keep protection of privacy afloat.[267] Greece is accordingly a good example and amongst the 'success stories' on how COVID-19 has been tamed without compromising data protection for it constantly promotes data security in its effort rather than encouraging excessive collection of data through e.g. using digital trackers.[268]

The COVID-19 outbreak have thereby made societies realize the need to be better prepared in responding to these kinds of crises – both in terms of action plans but also through legislation because it greatly impacts data rights, not to mention all areas of our societies and economies. Therefore, even though EU MS' cooperation is significant to overcome COVID-19. It requires

[263] EDPB, Guidelines 03/2020 (n 234); Finck and Pallas (n 263).
[264] Shachar and Others (n 242) 21; WHO, Guidance for Managing Ethical Issues in Infectious Disease Outbreaks (2016) <https://apps.who.int/iris/bitstream/handle/10665/250580/9789241549837-eng.pdf?sequence=1&isAllowed=y> accessed May 7 2021; Kimberlee Moran, 'Damned by DNA — Balancing personal privacy with public safety' [2018] E3-E4 FSI 292; The Lancet Respiratory Medicine (n 257).
[265] GDPR (n 7) Recital 2; Finck and Pallas (n 263) 34.
[266] EC, 'Shaping Europe's digital future: DSM' (n 200); EC, 'A Digital Single Market for the benefit of all Europeans' [2019] <https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53056> accessed May 7 2021.
[267] EC, 'Digital health technologies addressing the pandemic' <https://ec.europa.eu/digital-single-market/en/digital-health-technologies-addressing-pandemic> accessed May 4 2021; EC, 'Commission proposes new rules and actions for excellence and trust in Artificial Intelligence' <https://digital-strategy.ec.europa.eu/en> accessed May 3 2021.
[268] Vassilis Hatzopoulos, 'Taming the COVID-19, not the GDPR: the case of Greece' (*BlogDroitEuropeen*, 2020) <https://blogdroiteuropeen.com/2020/07/04/taming-the-covid-19-not-the-gdpr-the-case-of-greece-by-vassilis-hatzopoulos/> accessed May 5 2021; Stephanos Mitsios, 'GREECE COVID-19: How should Greek companies respond in compliance with the GDPR?' (*EY*, 2020) <https://www.ey.com/en_gr/tax/tax-alerts/greece-covid-19-how-should-greek-companies-respond-in-compliance-with-the-gdpr> accessed May 7 2021; GCT, 'MEP Eva Kaili: Greece Can Become The Next "success Story" Of Europe' <https://greekcitytimes.com/2020/12/30/kaili-greece-success-story-europe/> accessed May 5 2021; By Marianthi Hatzigeorgiou and Minakshi Raj, 'Why is Greece an outlier in EU's Covid-19 response?' (*EUObserver*, 2020) <https://euobserver.com/opinion/148397> accessed May 4 2021.

regulators to keep a close eye and govern these technologies and measures applied by organisations.

The personal data extracted from mobile phones, applications and other technologies are without doubt vital in such response, however, the responsible use of such data and aligning processing of such with current DPR is still of paramount importance to maintain public's trust. In failing to do so, citizens will disregard any advice, restrictions and recommendations from public health and other authorities resulting in adverse effects on their efforts to tackle COVID-19.[269] It is therefore notable that privacy challenges arising from COVID-19 are not merely of a technical nature, for it also has proven how fragile our communities are which challenges leaders and policymakers in their decisions.[270] The COVID-19 hence pushes the EU to put its citizens in the heart of its response rather than corporations – and to go an extra mile reinforcing strong democracies by making sure that citizen's rights e.g. protection of privacy are not hampered.[271]

Existing legislations such as GDPR must take into consideration the consequences of legitimizing restriction and whereas abuse of such legal bases happen – it may therefore call for stringent conditions that companies have to fulfil when processing personal data and a narrow interpretation of such exemptions in order to guarantee the highest privacy standards within the Union. This additionally conveys that preserving data protection primarily relies on legal frameworks, it also depends on authorities and those in power to promote such privacy enforcement and compliance through setting up data protection agendas in national level, overseeing companies in their use of current technologies to be better prepared in tackling more complex privacy issues in the future.[272]

The inclusion of digital privacy in a number of updated European and International strategies and regulatory approach (e.g. EU's IPCR, UN's Priorities for 2021,[273] ICO Technology Strategy,[274] and OECD Digital Economy Policy[275]) symbolizes that digitalization will not only play a key

[269] Marcello Ienca and Effy Vayena, 'On the responsible use of digital data to tackle the COVID-19 pandemic' [2020] 26 NATMED 463–464; Paul Ward, 'Improving Access to, Use of, and Outcomes from Public Health Programs' (*Frontiers*, 2017) <https://www.frontiersin.org/articles/10.3389/fpubh.2017.00022/full> accessed May 4 2021.
[270] Ibid.
[271] Ibid (n 193).
[272] Ibid.
[273] UN 'Report of the Secretary-General on the work of the Organization' GAOR 77th Session Supp No 1 UN Doc A/75/1 (2020); IISD, 'UN Secretary-General Presents 10 Priorities for 2021 Knowledge Hub' (SDGKH, 2021) <https://sdg.iisd.org/news/un-secretary-general-presents-10-priorities-for-2021/> accessed May 9 2021; António Guterres, 'Remarks to Member States on Priorities for 2021' (*UN*, 2020) <https://www.un.org/sg/en/content/sg/speeches/2021-01-28/remarks-member-states-priorities-for-2021> accessed May 9 2021.
[274] ICO, 'Technology Strategy 2018-2021' <https://ico.org.uk/media/about-the-ico/documents/2258299/ico-technology-strategy-2018-2021.pdf> accessed May 6 2021.
[275] OECD, Resolution of the Council renewing and revising the Mandate of the Committee on Digital Economy Policy, approved by the Council on 11 December 2018 at its 1387th session C/M(2018)24 ITEM 252.

role in a crisis like this but also in tackling other existing and societal issues our nations are facing today.[276] This means that although COVID-19 have accelerated digitalization and unfolded digital technologies potentials, these events have also demonstrated that privacy will be the top issue of the century as it trembles many areas of our lives, societies, and fundamental rights.

By having such strong sets of legal frameworks and consistent guidelines from policymakers, crises such as the COVID-19 that accelerated and exposed pose us to unprecedented privacy issues just might help data protection to survive more compound obstacles.[277] The ultimate way forward is to continuously preserve and improve DPR accordingly, and as privacy challenges persist it will demand better preparedness in responding to more complex challenges than just the question of whether data rights are hindering efforts to save lives.

[276] Council Implementing Decision (EU) 2018/1993 of 11 December 2018 on the EU Integrated Political Crisis Response Arrangements [2018] OJ L 320; EC, 'The EU Integrated Political Crisis Response' [2018] 195 RS <https://www.consilium.europa.eu/media/29699/web_ipcr.pdf> accessed May 7 2021; Iñigo Beriain and Others, 'The European Union Integrated Political Crisis Response Arrangements: Improving the European Union's Major Crisis Response Coordination Capacities' [2015] 9(3) Cambridge 234.

[277] Empower citizens for digital age (n 7); FRA, Your rights matter: data protection and privacy (n 201); Livia and Others (n 205); Wojciech Wiewiórowski, 'COVID-19' (EDPS, 2020) <https://edps.europa.eu/data-protection/our-work/subjects/covid-19_en> accessed April 29 2021; WHO, 'The Future of Digital Health Systems 2.0: safe and inclusive digital health for all' (2020) <https://ehealthresearch.no/whoisdigital2020> accessed May 7 2021.

# CHAPTER VI:
# ANALYSIS AND DISCUSSION

Digital technologies have transformed our ways of working, learning and how societies cope with crises which in turn makes disclosure of personal data an integral part of our lives. This in turn demands flexibility from the European privacy regimes to not govern technological developments but to also address other societal issues it brings along. The Union has acknowledged such challenges and has taken its stand through the adoption of GDPR, as well as other data protection rules to strengthen digital rights. However, such regulations have shown to be requiring consistent development to overcome stumbling blocks such as those presented by today's COVID-19 crisis. [278]

These developments on privacy regimes must also include enhanced pressure on different sectors, local governments and big tech companies to complement the data protection goals because processing of personal data will become a permanent component of our work and operations. This is particularly important today as the COVID-19 have advanced society's digital transition and require the public to operate in the comforts of their homes. Such accelerated digitalization increases exposure of our private life such as our living conditions, location and even those we live with. It additionally entails that collection and processing of personal data have macro scaled because apart from limited mobility, individuals are obligated to disclose personal information for these agencies to control the virus spread.[279]

For that reason, although the DPR provides an exhaustive list of lawful bases for processing personal data such as consent offered by Article 6 GDPR, there is a degree of drawback on this kind of provision. It should be recalled that Article 6 highlights that consent shall be freely given but in the COVID-19 context, the essence of the term 'freely' may not be satisfied because businesses or academic institutions that shifts to remote working may be subject its employees or students to certain requirements utilizing private devices and installing software that may in turn access an individual's highly personal data. This means that although technologies such as Zoom's and Google reassures that adequate data protection are set up for users (e.g. use of a unique identifier or randomized digits as login information or network perimeters) these forms of tools have nevertheless proven to experience data intrusions resulting to data thefts and leaks.[280]

[278] Chapters 1 and 4.
[279] Ibid; Chapter 2, Sections 3.2 and 4.1
[280] Ibid.

As a further matter, since the GDPR acknowledges emergency situations such as COVID-19 as an exemption to restring data rights and process personal or sensitive data, it frees controller and processor from obtaining data subjects' consent. Whilst these forms of provisions are necessary to balance both interests, it additionally implies that little to no control or genuine choice of declining such processing are offered to data subjects. Be that as it may, the uncertainty and challenging time our citizens are experiencing today comes with the need to feel safe. Hence, preserving data subject's power over one's personal data can provide reassurance and ensure that data subjects are informed of the purposes of processing – enabling data subjects to play an active role in digital transition and shaping the digital future.[281]

The current EU DPR are thus fronted with the challenge to maintain data protection enforcement and to closely govern developing technologies, as well as organisation data processing operations to maintain EU privacy standards because these privacy regimes are now not only tested by digital acceleration but as by a global health crisis. Moreover, there are debates on whether the opportunities to lawfully restrict data protection under Article 9 and 89 GDPR are at risk of exploitation because tech giant companies may hide their misuse of data through the 'emergency situation' facade offered by these provisions. Hence, this demands DPA to pay a closer look into digital solutions that are claimed necessary to fight the pandemic. While the DPA needs to prevent abuse of such regimes, it should, although carefully take into consideration the apportionment of responsibilities between these parties in assessing data breaches so that companies are not completely dissuaded from utilizing digital technologies in a crisis like this.[282]

A greater emphasis on how health and other sensitive data are to be handled was the focus of Guidelines 03/2020 for purposes of scientific researchers is a crucial component of EUDPR because the interpretation of the concept of 'scientific research' is not explicitly defined by the GDPR, this Guideline explains that such concepts cover technological development, and demonstration, fundamental research, applied research and privately funded research. The broadness of the concept gives room for wide varieties of digital solutions to fall under the special regime clause. However, the EDPS pointed out that processing data for research purposes often follows strict ethical standards apart from GDPR.

This concept therefore not only indicates current DPR's flexibility but safeguards responsible use of special regime or exemptions clauses because entities are obligated to handle and manage these data in good faith, to

[281] Sections 2.1-2 and 5.1
[282] Ibid.

improve security practices, as well as to carefully consider data protection risks that such a research project may inherits – more so in health-related research. The EU hence explicitly emphasized that Article 89 GDPR must not be understood as a tool for entities to escape its privacy obligations and liabilities during a time like this.[283]

On the other hand, the scope of concepts such as 'research purposes' or 'public interest' mentioned in these provisions remain to require clarifications from the DPA and ethical review boards. By doing so, companies will be forced to be diligent and explicitly lay out its intentions for conducting such research projects and the processing means it pursues. These agencies must agree on activities falling under research purposes that embody genuine objective of serving the public good. Such common understanding on these concepts could sequentially set out limitations, avoid the consequences arising from misuse of these clauses, positively impact how these sensitive data are processed, and meet the objectives of general interest acknowledged by the Union.[284]

The establishment of good privacy practices with regards to processing of personal data, more so with sensitive data, further heightens the bar for other countries outside the EU borders. This is particularly significant in the context of digitalization and COVID-19 because data sharing and transfers are necessary to develop treatments, vaccines and other preventive medicines. It will particularly allow organisations to reflect upon privacy and security practices when working with other third country processors or using cloud to manage their data. Although the EU is yet to come up with a solution for EU-US or third country data transfers after invalidating the Safe Harbour and Privacy Shield, different sectors are now paying more attention on what the upcoming privacy framework will look like and preparing themselves to improve their data processing activities and management.[285]

As the COVID-19 battle demands massive amounts of data, many data processing and transfers are additionally based on Article 89 GDPR and 49 (1) GDPR that is necessary for public interest in the area of public health. On the other hand, Guideline 03/2020 makes clear that derogation clauses are to be strictly interpreted and must be assessed on a case-by-case basis. That being the fact, entities must one way or another consider setting up adequate safeguards when processing and transferring sensitive data outside the EU. The invalidation of EU-US privacy frameworks more signifies that current EU privacy regimes require a high level of security and technical measures on entities processing EU citizens data. Hence, data protection should not be

[283] Chapter 4 and Section 5.1.
[284] Sections 2.2 and 5.2.
[285] Ibid; and 3.1.

compromised, and derogation clauses are similarly not to be used to breach fundamental rights. It also signals that such clauses solely serve to accommodate emergency or exceptional situations – and strict interpretation of such will put pressure on organizations to go an extra mile in fully understanding who can benefit from these provisions and to what extent.[286]

These ongoing events have indeed unravelled many privacy concerns in relation to digitalization leaving advocates wondering whether the GDPR is ready for these kinds of threats or whether it is simply too early to question the Regulation's power because even though it has only been enforced for three years, it has proven to be resilient these two events. Notwithstanding, scholars and privacy regulators pointed out that a number of in demand digital technologies today have existed before GDPR which entails that these do not particularly embed or meet the current privacy standards. Apart from the current EUDPR, it is thus crucial to move forward with digital frameworks and agendas guaranteeing a safer and healthier digital life; as well as to answer current privacy questions such as the limits of processing of sensitive data and address technologies that are not successfully achieving the purpose pursued. [287]

To put into context, the use of digital technologies to support the COVID-19 make collecting and processing of personal data necessary. However, such necessity does not automatically guarantee that these will produce effective results to the purpose achieved like the Apple-Google tracing application mentioned earlier. Such a debate is important not only because these solutions process amongst the most sensitive data, but it can constrain organisations to carefully evaluate the forms of technologies implemented. This is particularly even more vital because these data are shared between sectors and outside the European borders – similarly as the S*chrems* judgments suggest. On the assumption that effectiveness does not count as a criterion under special regime or the concept of necessity, another layer of protection shall instead be guaranteed to these personal data such as pseudonymisation or other more sophisticated security as suggested by Article 89 GDPR rather than unique identifiers similar to Zoom's.[288]

There is indeed no clear evidence that by imposing stringent conditions and perimeters for processing of personal data on the basis of the special regime or exemption clauses offered by the will indeed save lives. Notwithstanding, the way technologies depend on personal data to function indicates that data protection plays a very crucial role in both of these contexts. The processing of personal data as part of COVID-19 response is thus unavoidable because

[286] Sections 2.1, 3.1, and 5.2.
[287] Chapter 2, Sections 5.2 and 3.2.
[288] Ibid; and 3.1.

it helps us gather as much information regarding the live state of virus cases and its spread. In safeguarding that accelerated digitalization and COVID-19 will be manageable for authorities, bearable for individuals and not obstruct societies, there is a possibility that the future may demand the right to privacy to be absolute or for the reasonable restrictions on such right to be narrow.[289]

The EU has repeatedly pointed out that existing data protecting rules remain enforced and so privacy is to be preserved but such a statement does not explicitly guide entities in guaranteeing fair balance of privacy with other interests. It is also worth noting that such balance is interchangeable as the current situation remains unsettled. The European privacy regime is indeed presented with a lot of stumbling blocks which in some way forces privacy frameworks to advance, and for regulators to reflect upon current and future issues it will have to address. The aforesaid Guidelines are nevertheless vital components of existing DPR that facilitates and clarifies the limits of data protection provisions. Although it is too early to scrutinize the success of these privacy frameworks, new regulatory frameworks such as DMA and DSA can intensify and assist existing privacy regimes to overcome these privacy issues and tests.[290]

All things considered, the European privacy regime exhibits its ability to address such unprecedented event, as well as it has demonstrated adaptability to the measures taken to safeguard the common good through e.g. enforcement of a special regime, derogations, guidelines, and by enabling MS to implement legal measures that it presumes necessary to tackle the pandemic. While accelerated digitalization and the Coronavirus crisis are two unknown and complex territories, the current data protection rules and its principles remain steadfast in an uncertain time. The current European privacy regime also proves that, rather than hindering efforts made to overcome the challenges these bring, it is a vital tool that strengthen citizen's digital rights, the convergence of economies within the EU internal market, as well as shapes digitalization so that societies and economies can positively benefit from it. Finally, these legal frameworks are most certainly a reminder that the European data protection remains enforced and persistent.

[289] Chapter 1-3, Openings and Section 5.1.
[290] Ibid.

# CHAPTER VII:
# CONCLUSION

These two current events have made citizens question many aspects of our societies and how it is governed because digitalization and COVID-19 are two phenomena that have direct impact on our fundamental rights such as the right to data protection. Nevertheless, the GDPR and other European privacy regimes set out that the aim to empower data subjects' rights is being achieved because these frameworks positively altered how organisations manage EU citizen's personal data, and correspondingly enabled harmonisations of privacy standards across Europe. As a result, controllers or processors, located within or outside the Union, are given enhanced duties and obligations to facilitate the GDPR's objectives. In that manner, privacy challenges that arise from increasing dependency on digital transformation and technologies will not be impossible overcome because special attention remains to be given on supplementing the GDPR objectives with digital agenda, strategies and new policies.

Notwithstanding, these events have shown to require leaders and policymakers to better understand these different digital technologies that can assist them in their decisions. It is similarly vital for data subjects to have such knowledge to ensure continuous realization of such rights. The COVID-19 crisis on the other hand have presented complex challenges on the data protection regimes because it has accelerated digitalization more than ever; and particularly posing threats on privacy because communities are coerced to shift to digital form. For that reason, such a crisis has presented the value of utilizing digital technologies and processing personal data in such a battle. With this mind, some perceive that data protection rules are an obstacle in the race to save lives from this infectious disease.

On the contrary, the EU and other data protection authorities have reassured that the COVID-19 is a shared crisis that also presents threats on citizen's fundamental rights. The European privacy regime role is therefore not only essential to safeguard such rights but also to overcome privacy challenges arising from such crises that may leave a detrimental impact on our lives, communities and the internal market. To that end, the current European privacy regime is established to drive these technologies to a path that benefits us all. Hence, such regime does not in any means hinder COVID-19 efforts or digital developments but rather reveals that privacy will be one of the next top issues of the century – making protection of personal data a must in alleviating harms arising from these events.

# TABLE OF LEGISLATIONS

## *I. EUROPEAN UNION LAW*

### LEGISLATIONS

Charter of Fundamental Rights of the European Union (adopted 2 October 2000, entered into force 7 December 2000) OJ C 326/291 (Charter of the Fundamental Rights)

Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union (TFEU) [2016] OJ C202/1

European Convention for the Protection of Human Rights and Fundamental Freedoms (adopted 4 November 1950, entered into force 3 September 1953) ETS 5 (ECHR)

Regulation (EC) 1338/2008 of the European Parliament and of the Council of 16 December 2008 on Community statistics on public health and health and safety at work (Public Health Statistics) OJ L 354/70

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 free movement of such data and repealing Directive 95/46/EC (GDPR) OJ 2016 L 119/1

### CASE LAWS

Case C-101/01 *Bodil Lindqvist* [2003] ECR I-12971

Case C-131/12 *Google Spain and Google* [2014] EUC 317

Case C-136/17 *GC and Others v Commission nationale de l'informatique et des libertés* (CNIL) [2019] ECLI 773

Case C-210/16 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH* [2016] ECLI 388

Case C-311/18 *Data Protection Commissioner v Facebook Ireland Ltd* (Schrems II) [2020] ECLI 559
Case C-362/14 *Maximillian Schrems v Data Protection Commissioner* (Schrems I) [2015] ECLI 650

Case C-40/17 *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV* (Fashion ID) [2019] ECLI 629

Case C-507/17 *Google LLC v Commission nationale de l'informatique et des libertés* [2019] ECLI 257

Joined Cases C-468/10 and C-469/10 *Asociación Nacional de Establecimientos Financieros de Crédito* (ASNEF) *and Federación de Comercio Electrónico y Marketing Directo* (FECEMD) *Administración del Estado* [2011] ECLI 777

### DIRECTIVES AND DECISIONS

Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce [2000] OJ L 215

Council Directive 95/46/EC 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 [1995] OJ L 281/31

Council Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L 201 (EPD)

Council Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare [2011] OJ L 88

Council Directive 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information [2019] OJ L 172

Council Implementing Decision (EU) 2018/1993 of 11 December 2018 on the EU Integrated Political Crisis Response Arrangements [2018] OJ L 320

# SOFT LAWS

## *EUROPEAN COMMISSION*

EC, Communication from the Commission Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection (2020) OJ C 124I

EC, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions A Digital Agenda for Europe (2010) COM(2010)245 final (EU Digital Agenda)

EC, 'Europe 2020: A European strategy for smart, sustainable and inclusive growth' [2020] COM/2010/2020 final (Europe 2020)

## *COURT OF JUSTICE OF THE EUROPEAN UNION*

CJEU, Press Release No 99/19 on Case C-40/17 (2019)

CJEU, Press Release No 103/18 on Case C-25/17 (2018)

## *EUROPEAN PARLIAMENT*

EP, 'The CJEU judgment in the Schrems II case' [2020] EPRS PE 652 073

European Parliamentary Research Service (EPRS), 'How the General Data Protection Regulation changes the rules for scientific research' [2019] PE 634.447

Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act) COM(2020)842 final

## *EUROPEAN DATA PROTECTION BOARD*

EDPB, Guidelines 03/2019 on Processing of Personal Data through Video Devices (2020)

EDPB, Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak (adopted 21 April 2020)

EDPB, Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak (adopted 21 April 2020)

EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR (adopted 2 September 2020) Guidelines 07/2020

EDPB Statement on the processing of personal data in the context of the COVID-19outbreak' (Adopted on 19 March 2020)

## *EUROPEAN DATA PROTECTION SUPERVISOR*

EDPS, Opinion 29 September 2008 on the notification for prior checking from the Data Protection Officer of the European Maritime Safety Agency regarding the "Recruitment of permanent, temporary and contract agents" (Case 2008-384)

EDPS, Opinions 10 February 2021 on the Digital Services Act and the Digital Markets Act (2021) EDPS/2021/02 (Opinions on DSA and DMA)

EDPS, Opinion 12 September 2011 on the updated notification concerning administrative inquiries and disciplinary proceedings within the Court of Justice of the EU (Case 2011-0806)

EDPS, Opinion 20 November 2017 10/2017 on safeguards and derogations under Article 89 GDPR in the context of a proposal for a Regulation

EDPS, Shaping a Safer Digital Future: The EDPS Strategy 2020 - 2024 (2020) EU (2020 Digital Strategy)

## *ARTICLE 29 WORKING PARTY*

Article 29 Working Party (A29WP) Guidelines on consent under Regulation 2016/679 (adopted on 28 November 2017, as last revised and adopted on 10 April 2018) 17/EN (Article 29 on consent) pages 3-5

A29WP, Opinion 1/2010 on the concepts of 'controller' and 'processor' (adopted on 15 February 2010) 00264/10 WP 169 (Article 29 on controller and processor)

A29WP, Opinion of the European Data Protection Supervisor on the data protection reform package [2012] C 192/7

A29WP, Advice paper on special categories of data ("sensitive data") [2012] ARES 444105

## *II. INTERNATIONAL AND NATIONAL LAW*

# INTERNATIONAL LEGISLATIONS


Statute of the International Court of Justice (adopted 26 June 1945, entered into force 24 October 1945) 1 UNTS XVI

Vienna Convention on the Law of Treaties (adopted 25 May 1969, entered into force 27 January 1980) 1155 UNTS 331 (Vienna Convention)


# INTERNATIONAL SOFT LAW


ILO, 'An employers' guide on working from home in response to the outbreak of COVID-19' [2020] < https://www.ilo.org/wcmsp5/groups/public/---ed_dialogue/---act_emp/documents/publication/wcms_745024.pdf > accessed May 1 2021, 14-16

OECD, Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (adopted 23 September 1980, amended 11 July 2013) C(80)58/FINAL, section 13 (d)

OECD, Resolution of the Council renewing and revising the Mandate of the Committee on Digital Economy Policy, approved by the Council on 11 December 2018 at its 1387th session C/M(2018)24 ITEM 252

UN 'Report of the Secretary-General on the work of the Organization' GAOR 77th Session Supp No 1 UN Doc A/75/1 (2020)


# NATIONAL LAW


USA Privacy Act of 1974 (approved and effective 31 December 1974) PL 93-579

USA Family Educational Rights and Privacy Act (FERPA) of 1974

USA Health Insurance Portability and Accountability Act (HIPAA) of 1996

UK Coronavirus Act 2020 Chapter 7

The Public Access to Information and Secrecy Act (2009:400) (PAIS) tom SFS 2021:82 Chapter 5

Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning SFS 2020:152

# TABLE OF SOURCES

## I. LITERATURE


Banakar R and Travers M, Theory and Method in Socio-legal Research (Hart Publishing 2005)

Calder A, *EU GDPR Pocket Guide* (2edn, IT Governance Publishing 2018)

Creutzfeldt N and Others, *Routledge Handbook of Socio-Legal Theory and Methods* (Routledge 2019)

Galligan D, *Law in Modern Society* (OUP 2006)

Hart H L A, *The Concept of Law* (2nd edn, Oxford Clarendon, 1994)

Hoecke V, *Methodologies of legal research: what kind of method for what kind of discipline?* (Hart Oxford 2011)

Jay R, *Guide to General Data Protection Regulation* (4edn, Thomson Reuters 2017)

Levene M, *An Introduction to Search Engines and Web Navigation* (1st edn, Somerset Wiley (2011)

Linder A, *European Data Protection Law: General Data Protection Regulation* (EU 2016)

Möllers T M J, *Legal Methods* (Beck and Hart Publishing, 2020)

Reid P and Others, *Building a Better Delivery System: A New Engineering/Health Care Partnership* (NAP 2005)

Dagmar Rosenbrand and Others, *Risk Classification of Data Transfer in Medical Systems. Computer Safety, Reliability, and Security* (Springer 2015)

Rowland D and Others, *Information Technology Law* (4edn, Routledge 2012)

Slokenberga S and Others, *GDPR and Biobanking* (1st edn, Springer 2021)

US Department of Justice, *Guide to the Freedom of Information Act* (DOJ FOI 2020)

Weber M, *Economy and Society* (University of California Press 1968)

White Case, *Unlocking the EU General Data Protection Regulation: A practical handbook on the EU's new data protection law* (White Case LLP 2019)

# II. EUROPEAN UNION DOCUMENTS


A29WP, Letter to clarify the scope of the definition of data concerning health (5 February 2015) 1–2 <https://ec.europa.eu/justice/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_en.pdf> accessed April 28 2021

DigitalEurope, 'Two years of GDPR: A report from the digital industry' [2020] DE 1 <https://www.digitaleurope.org/wp/wp-content/uploads/2020/06/DIGITALEUROPE_Two-years-of-GDPR_A-report-from-the-digital-industry.pdf> accessed January 19 2021

Dumbrava C, 'Lifting Coronavirus Restrictions' [2020] EPRS 652.016 <https://op.europa.eu/en/publication-detail/-/publication/24f80771-d143-11ea-adf7-01aa75ed71a1/language-en> accessed May 7 2021

EC, 'Assessment of the EU Member States' rules on health data in the light of GDPR' <https://ec.europa.eu/health/sites/health/files/ehealth/docs/ms_rules_health-data_en.pdf> [2021] DGHS accessed May 5 2021

EC, 'Commission proposes new rules and actions for excellence and trust in Artificial Intelligence' <https://digital-strategy.ec.europa.eu/en> accessed May 3 2021

EC, 'DG Information Society and Media at a Glance' [2006]

EC, 'Digital health technologies addressing the pandemic' <https://ec.europa.eu/digital-single-market/en/digital-health-technologies-addressing-pandemic> accessed May 4 2021

EC, 'EU Budget for the Future' [2018] <https://euagenda.eu/upload/publications/untitled-199893-ea.pdf> accessed March 30 2021

EC, 'Promoting Europe's interest and protecting European Values in the Global Digital Transformation' [2019] <https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=61697> accessed March 28 2021

EC, 'Special Eurobarometer 487a Report; The General Data Protection Regulation' [2019] EC

EC, 'The EU Integrated Political Crisis Response' [2018] 195 RS <https://www.consilium.europa.eu/media/29699/web_ipcr.pdf> accessed May 7 2021

EC, 'The GDPR: new opportunities, new obligations' [2018] EU Luxembourg <https://ec.europa.eu/info/sites/info/files/data-protection-factsheet-sme-obligations_en.pdf> accessed February 20 2021

EC, 'Two years plan of the eHealth Network meetings and sustainability' [2019] V1.3 <https://ec.europa.eu/health/sites/health/files/ehealth/docs/ev_20190611_co512_en.pdf> accessed May 2 2021

ECDC, 'Data on country response measures to COVID-19' [2021] <https://www.ecdc.europa.eu/en/publications-data/download-data-response-measures-covid-19> accessed April 22 2021

EDPS, 'Annual Report 2020' [2021] EU

EDPS, 'The GDPR for EU institutions: your rights in the digital era 2019' [2018] EDPS <https://edps.europa.eu/sites/default/files/publication/18-12-11_factsheet1_your_rights_in_digital_era_en_2.pdf> acessed January 17 2021

EESC, 'Digitalisation: challenges for Europe' [2019] EESC 80-87

EP, 'Digital Agenda for Europe' [2021] EU EP <https://www.europarl.europa.eu/ftu/pdf/en/FTU_2.4.3.pdf> accessed March 11 2021

EPRS, 'Upholding human rights in Europe during the pandemic' (2020) <https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/652085/EPRS_BRI(2020)652085_EN.pdf> accessed March 18 2021

Fuster G, 'Big Data and Smart Devices and their Impact on Privacy' (EP, 2015) <https://www.researchgate.net/profile/Gloria-Gonzalez Fuster/publication/289538954_Big_Data_and_Smart_Devices_and_their_Impact_on_Privacy/links/568ff7ce08aec14fa557b70b/Big-Data-and-Smart-Devices-and-their-Impact-on-Privacy.pdf> accessed April 14 2021

# III. JOURNAL ARTICLES


Alsenoy B V, 'Liability under EU Data Protection Law' [2016] JIPITECT 271

Arabo A and Others, 'Privacy in the Age of Mobility and Smart Devices in Smart Homes' [2012] IEEE 819

Ausloss J and Others, 'Getting Data Subject Rights Right A submission to the European Data Protection Board from international data rights academics, to inform regulatory guidance' [2020] 10(3) JIPITEC 283

Baig A and Others, 'The COVID-19 recovery will be digital: A plan for the first 90 days' [2020] McKinseyDigital 1

Becker R,'COVID-19 Research: Navigating the European General Data Protection Regulation' [2020] 22(8) JMIR E19799

Beriain I and Others, 'The European Union Integrated Political Crisis Response Arrangements: Improving the European Union's Major Crisis Response Coordination Capacities' [2015] 9(3) Cambridge 234

Boudreaux B and Others, 'Data Privacy During Pandemics: A Scorecard Approach for Evaluating the Privacy Implications of COVID-19 Mobile Phone Surveillance' [20202] RAND

Bradford L, 'COVID-19 contact tracing apps: a stress test for privacy, the GDPR, and data protection regimes' [2020] 7(1) JLB 1

Cotterrell R, 'The Sociological Concept of Law' [1983] 10(2) JSTOR 241

Dannenberg P and Others, 'Digital Transition by COVID-19 Pandemic?' [2020] 111(3) TESG 543-560

DataStreams IO, 'GDPR Obligations on data processors' [2019] DSIO

Devi R and Others, 'A study on impact of electronic devices on youngsters' [2019] 8(5) The Pharma Innovation Journal 283-292

Ellickson R C, 'Order without Law: How Neighbors Settle Disputes' [1991] Harvard University Press

Emanuele Ventrella, 'Privacy in emergency circumstances: data protection and the COVID-19 pandemic' [2020] ERA Forum 21, 379

Faraj S and Others, 'Unto the breach: What the COVID-19 pandemic exposes about digitalization' [2021] 31(1) McGill University 100337

Finck M and Pallas F, 'They who must not be identified—distinguishing personal from non-personal data under the GDPR' [2015] 10(1) IDPL 34

Globocnik J, 'The Right to Be Forgotten is Taking Shape: CJEU Judgments in GC and Others (C-136/17) and Google v CNIL (C-507/17)' [2020] 69(4) GRUR International 380

Guhr N and Others, 'Privacy concerns in the smart home context' [2020] 2 SN Appl. Sci 247

Ienca M and Vayena E, 'On the responsible use of digital data to tackle the COVID-19 pandemic' [2020] 26 NATMED 463

Introna L, 'Privacy and the Computer: Why We Need Privacy in the Information Society' [1997] 28(3) Blackwell 259

Kapur R, 'Significance of Digital Technology' [2018]

Kedzior M, 'The right to data protection and the COVID-19 pandemic: the European approach' [2020] 21 ERA 533-543

Kolfschooten H V and Ruijter A K, 'A legal perspective on contact tracing' [20202] 41(3) CSP 478

Lind R, 'The new general data protection regulation—where are we are and where might we be heading?' [2015] 14 Springer 95-100

Linden T and Others, 'The privacy policy landscape after the GDPR' [2019] Scienda 1-18

Lucivero F and Others, 'COVID-19 and Contact Tracing Apps: Technological Fix or Social Experiment?' [2020] 1 SSRN

Marelli L and Others, 'Fit for purpose? The GDPR and the governance of European digital health' [2020] 41(5) Policy Studies 447

Mascalzoni D, ‘Ethics, law and governance of biobanking’ [2015] 14(1) Springer 53-77

Masur P K, ‘How Online Privacy Literacy Supports Self-Data Protection and Self-Determination in the Age of Information’ [2020] 8(2) COGITATIO 258–269

McLennan S, ‘COVID-19: Putting the General Data Protection Regulation to the Test’ [2020] 6(2) JMIR E19279

Moran K, ‘Damned by DNA — Balancing personal privacy with public safety’ [2018] E3-E4 FSI 292

Mourjo Sen and Others, ‘Issues of Privacy and Security in the Role of Software in Smart Cities’ [2013] ICCSNT

Murdoch S and Kapadia A, ‘PoPETs’ [2020] 4 Sciendo, 47–64

Nesterchuk O A and Others, ‘Digitalization as the "new normal" of higher education’ [2020] 1691(1) Journal of physics 12068

Olsen C, ‘To track or not to track? Employees’ data privacy in the age of corporate wellness, mobile health, and GDPR’ [2020] 10(3) IDPL 236-252

Puljak L and Others, ‘Before and after enforcement of GDPR’ [2020] 30(3) BiochemMed 030201

Rohmann K and Others, ‘Digital Transformation in the EU 2035 A Glimpse into the Future’ [2019] 7 Deloitte

Sandgren C, ‘Är rättsdogmatiken Dogmatisk?’ (2008) 118(4-5) Tidsskrift for Rettsvitenskap 650

Shachar C and Others, ‘AI Surveillance during Pandemics: Ethical Implementation Imperatives’ [2020] THC 50(3)

Sharon T, ‘Blind-sided by privacy? Digital contact tracing, the Apple/Google API and big tech’s newfound role as global health policy makers’ [2020] EIT 1-3

Schneider G, ‘Disentangling health data networks’ [2019] 9(4) IDPL 267–271

Schäffer B, ‘The Digital Literacy of Seniors’ [2007] 2(1) Universität der Bundeswehr

Selwyn N, ‘What’s the problem with learning analytics?’ [2020] 6(3) JLA 1

Stucke M E, ‘Is competition always good?’ [2017] 1(1) JAE 163

Svenskt Näringsliv, ‘Position Paper: Digital Services Act’ [2020] SN 1

Svensson M and Others, ‘Digitalization and Privacy: A systematic literature review’ [2016] Lund University

Tene O, ‘What Google Knows: Privacy and Internet Search Engines’ [2008] 1433 WestLaw

Teräs M and Others, ‘Post-Covid-19 Education and Education Technology ‘Solutionism’: A Seller’s Market’ [2020] 2 PSE 863

The Lancet Respiratory Medicine, ‘Data protection: balancing personal privacy and public health’ [2015] 4(1) LRM 1

Uddin S and Others, ‘Onslaught of COVID-19: How Did Governments React and at What Point of the Crisis?’ [2021] 24(1) PHM 1

Wachter S and Mittelstadt B, ‘A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI’ [2019] 2(1) CBLR 461

Wallis K and Others, ‘Research using electronic health records: Balancing confidentiality and public good’ [2018] 10(4) JPHC 288

Zaeem R and Others., ‘The Effect of the GDPR on Privacy Policies: Recent Progress and Future’ [2020] 12(1) ACM 14-18

Ziani A and Medouri A, ‘Cloud Computing: Security and Privacy Issues’ [2019] 2 Springer

# IV. ONLINE ARTICLES


Bican P M and Brem A, 'Digital Business Model, Digital Transformation, Digital Entrepreneurship: Is There A Sustainable "Digital"?' [2020] MDPI <https://www.researchgate.net/publication/342580682_Digital_Business_Model_Digital_Transformation_Digital_Entrepreneurship_Is_There_A_Sustainable_Digital/fulltext/5efbe5e5299bf18816f5f3c1/Digital-Business-Model-Digital-Transformation-Digital-Entrepreneurship-Is-There-A-Sustainable-Digital.pdf> accessed March 7 2021

Bock K and Others, 'Data Protection Impact Assessment for the Corona App' [2021] 1(6) FIfF 46 <https://www.researchgate.net/publication/348618489_Data_Protection_Impact_Assessment_for_the_Corona_App/fulltext/6007a065a6fdccdcb868a2f6/Data-Protection-Impact-Assessment-for-the-Corona-App.pdf> accessed April 29 2020

Bunker B, 'A Summary of International Reports, Research and Case Studies of Digital Literacy' [2010] NZCS <https://itp.nz/files/201001%20Digital%20Literacy%20Research%20Report.pdf> accessed March 29 2021

Chakraborty I and Maity P, 'COVID-19 outbreak: Migration, effects on society, global environment and prevention' [2020] ScienceDirect <https://doi.org/10.1016/j.scitotenv.2020.138882> accessed January 26 2021

Dans E, 'Innovation, the Future of Society and People' [2019] Medium <https://www.enriquedans.com/wp-content/uploads/2019/11/Indra_Dans_ing.pdf> accessed March 10 2021

Deloitte, 'A new era for privacy: GDPR Six Months On' [2018] Deloitte LLP <https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/risk/deloitte-uk-risk-gdpr-six-months-on.pdf> 6 accessed February 27 2021.

Deloitte, 'Data privacy in the cloud' <https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/risk/ca-en-risk-privacy-in-the-cloud-pov.PDF> accessed April 10 2021

Deloitte, 'Privacy and Data Protection in the age of COVID-19 Download brochure' [2020] Deloitte 1 <https://www2.deloitte.com/content/dam/Deloitte/be/Documents/risk/be-risk_privacy-and-data-protection-in-the-age-of-covid-19.pdf> accessed January 28 2021

Dhaini A and Others, 'Covid-19 as accelerator of digital transformation' [2020] KPMG 1 <https://assets.kpmg/content/dam/kpmg/sa/pdf/2020/covid-19-as-accelerator-of-digital-transformation-and-the-gig-economy.pdf> accessed February 1 2021

EY 'GDPR: Demanding New Privacy Rights and Obligations' [2017] <https://eyfinancialservicesthoughtgallery.ie/wp-content/uploads/2017/11/ey-gdpr-demanding-new-privacy-rights-and-obligations-1_Optimized_Optimized.pdf> accessed February 23 2021

FTMS, 'Computing Basics' [2019] CSCA0101 <https://ftms.edu.my/v2/wp-content/uploads/2019/02/csca0101_ch07.pdf> accessed April 18 2021

Green L, 'The Concept of Law Revisited' 96(6) MLR <https://repository.law.umich.edu/mlr/vol94/iss6/15> accessed February 4 2021

GovTech, 'OECD to develop principles for govt access to private data; Protecting Personal Data in a Pandemic' (*GT*, 2021) <https://docs.google.com/document/d/1oqHklGOC3eRTVphjMKMiMqZnKs5MCuKo/edit#> accessed May 2021

HealthManagement, 'European Commission Announces Digital Agenda for Europe' [2010] 10(3) HM <https://healthmanagement.org/pdf/article/european-commission-announces-digital-agenda-for-europe> accessed March 16 2021

IApp, 'The California Privacy Rights Act of 2020' [2020] <https://iapp.org/resources/article/the-california-privacy-rights-act-of-2020/> accessed May 5 2021

Interact, 'Data management, privacy, and security in connected systems' [2018] Signify <https://www.interact-lighting.com/b-dam/b2b-li/en_AA/interact/articles/data-management/interact-sec-wp.pdf> accessed April 19 2021

Koevoets D, 'The Influence of Article 89 GDPR on the Use of Big Data Analytics for the Purpose of Scientific Research' [2015] TU <http://arno.uvt.nl/show.cgi?fid=142885> accessed May 6 2021

Laberge L and Others, ‘How COVID-19 has pushed companies over the technology tipping point—and transformed business forever’ [2020] McKinsey & Company 1 <https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/how-covid-19-has-pushed-companies-over-the-technology-tipping-point-and-transformed-business-forever> accessed January 26 2021

Lister R, Employee monitoring during the COVID 19 lockdown GDPR considerations revisited’ [2020] R&G <https://www.ropesgray.com/-/media/Files/alerts/2020/05/20200504_COVID_London_Alert.pdf> accessed May 2021

LTP, ‘A Regional Guide to Employee Data Privacy’ [2018] <https://www.leetsai.com/wp-content/uploads/2018/12/Regional-Guide-to-Employee-Data-Privacy-Asia-2018-LTP.pdf> accessed May 5 2021

Ministry of Education Government of India (MHRD), ‘Legal Research Methodology: Socio-legal Research’ [2019] MHRD <http://epgp.inflibnet.ac.in/epgpdata/uploads/epgp_content/law/09._research_methodology/04._socio-legal_research/et/8151_et_et.pdf> accessed February 4 2021

NCB, ‘Guide to the Ethics of Surveillance and Quarantine for Novel Coronavirus’ <https://www.nuffieldbioethics.org/assets/pdfs/Guide-to-the-ethics-of-surveillance-and-quarantine-for-novel-coronavirus.pdf> accessed May 4 2021

OCR, ‘Summary of the HIPAA Privacy Rule’ [2020] <https://www.hhs.gov/sites/default/files/privacysummary.pdf> accessed May 5 2021

Reddy A. and Vance A., ‘Student Privacy during the Pandemic’ [2020] AASA <https://iapp.org/media/pdf/resource_center/fpf_student_privacy_during_covid_19_pandemic.pdf> accessed May 3 2021

Rizzolo M K, ‘12 Reasons Why Data is Important’ [2020] CQL <https://www.c-q-l.org/resources/guides/12-reasons-why-data-is-important/#:~:text=Data%20allows%20organizations%20to%20more,locations%2C%20departments%2C%20and%20systems> accessed February 9 2021

Senarath A and Arachchilage N, ‘Why developers cannot embed privacy into software systems?’ [2018] EASE <https://arxiv.org/pdf/1805.09485.pdf> accessed April 5 2021

Sillitto H G, ‘Defining "System’’’ [2017] 27 INCOSE https://www.researchgate.net/profile/Scott-Jackson-13/publication/318601827_Defining_System_a_Comprehensive_Approach/links/597282b3458515e26dfd9517/Defining-System-a-Comprehensive-Approach.pdf> accessed April 18 2021

Ward P, ‘Improving Access to, Use of, and Outcomes from Public Health Programs’ (*Frontiers*, 2017) <https://www.frontiersin.org/articles/10.3389/fpubh.2017.00022/full> accessed May 4 2021

Wilson M and Others, ‘The implications of digitalization on business model change’ [2020] Innovation Engineering CIRCLE, <https://arxiv.org/pdf/2004.08937.pdf> accessed January 23 2021

Wright G W, ‘Hart's Concept of Law: Positivist Legal Theory or Sociology?’ [2010] SPP <https://www.researchgate.net/publication/262566886_Hart's_Concept_of_Law_Positivist_Legal_Theory_or_Sociology> accessed February 3 2021

Zanni T, ‘Investment in technology Innovation’ [2019] KPMG 1 <https://assets.kpmg/content/dam/kpmg/uk/pdf/2019/07/investment-in-technology-innovation.pdf> accessed January 19 2021

## V. ORGANISATION FOR ECONOMIC COOPERATION AND DEVELOPMENT


Lane M, 'Regulating platform work in the digital age' [2020] 1 OECD <https://goingdigital.oecd.org/toolkitnotes/regulating-platform-work-in-the-digital-age.pdf> accessed March 13 2021

OECD, 'COVID-19: Protecting people and societies' [2020] OECD <https://www.oecd.org/inclusive-growth/resources/COVID-19-Protecting-people-and-societies.pdf> accessed February 4 2021

OECD, 'Going Digital: Shaping Policies, Improving Lives' [2003] OECD <https://www.oecd.org/going-digital/going-digital-synthesis-summary.pdf> accessed March 27 2021

OECD, 'Policy Responses to Coronavirus (COVID-19): Ensuring data privacy as we battle COVID-19' [2020] OECD<https://read.oecd-ilibrary.org/view/?ref=128_128758-vfx2g82fn3&title=Ensuring-data-privacy-as-we-battle-COVID-19> accessed February 2 2021

Paunov C and Satorra S, 'How are digital technologies changing innovation?' [2019] OECD <https://www.researchgate.net/profile/Caroline-Paunov/publication/334593576_HOW_ARE_DIGITAL_TECHNOLOGIES_CHANGING_INNOVATION/links/5d337e8a92851cd04678a9b6/HOW-ARE-DIGITAL-TECHNOLOGIES-CHANGING-INNOVATION.pdf> accessed April 4 2021


## VI. WORLD HEALTH ORGANIZATION


WHO, 'Coronavirus' (WHO) <https://www.who.int/health-topics/coronavirus> accessed January 26 2021

WHO, 'Coronavirus disease (COVID-19): How is it transmitted?' (*WHO*, 2020) <https://www.who.int/emergencies/diseases/novel-coronavirus-2019/question-and-answers-hub/q-a-detail/coronavirus-disease-covid-19-how-is-it-transmitted> accessed January 27 2021

WHO, 'Digital tools for COVID-19 contact tracing' [2020] <https://apps.who.int/iris/rest/bitstreams/1279465/retrieve> accessed May 7 2021

WHO, 'The Future of Digital Health Systems 2.0: safe and inclusive digital health for all' (2020) <https://ehealthresearch.no/whoisdigital2020> accessed May 7 2021

WHO, Guidance for Managing Ethical Issues in Infectious Disease Outbreaks (2016) <https://apps.who.int/iris/bitstream/handle/10665/250580/9789241549837-eng.pdf?sequence=1&isAllowed=y> accessed May 7 2021


## VII. INFORMATION COMMISSIONER'S OFFICE


ICO, 'Guide to the General Data Protection Regulation' [2021] <https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf> accessed May 5 2021

ICO, 'Lawful basis for processing' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/> accessed February 12 2021

ICO, 'Smartphone security' <https://ico.org.uk/your-data-matters/online/smartphone-security/> accessed May 20 2021.

ICO, 'Technology Strategy 2018-2021' <https://ico.org.uk/media/about-the-ico/documents/2258299/ico-technology-strategy-2018-2021.pdf> accessed May 6 2021.

ICO, 'Updated regulatory approach in response to the coronavirus pandemic' [2020] 3(1) ICO


## VIII. DICTIONARY


'Software', *Techopedia* <https://www.techopedia.com/definition/4356/software> accessed April 17 2021

'Computer', *Techopedia* <https://www.techopedia.com/definition/4607/computer> accessed April 4 2021

'Digitalization', *Merriam-Webster Online* <https://www.merriam-webster.com/dictionary/digitalization> accessed January 24 2020

# IX. MISCELLANEOUS

## EUROPEAN UNION SOURCES


COE, 'Statement by Alessandra Pierucci and Jean-Philippe Walter' (2020) <https://www.coe.int/en/web/data-protection/statement-by-alessandra-pierucci-and-jean-philippe-walter> accessed May 6 2021

European Commission (EC), 'Commission report: EU data protection rules empower citizens and are fit for the digital age' (*EC* 2020) <https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1163> January 22 2021

EC, 'General Data Protection Regulation shows results, but work needs to continue' (*EC* 2019) <https://ec.europa.eu/commission/presscorner/detail/en/IP_19_4449> accessed February 12 2021

EC, 'General Data Protection Regulation: one year on' (*EC* 2019) <https://ec.europa.eu/commission/presscorner/detail/en/IP_19_2610> accessed February 13 2021

EC, 'How should requests from individuals exercising their data protection rights be dealt with?' (*EC*) <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/dealing-citizens/how-should-requests-individuals-exercising-their-data-protection-rights-be-dealt_en> accessed February 25 2021

EC, 'A Europe fit for the digital age' <https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_en#:~:text=The%20EU%27s%20digital%20strategy%20aims,this%20Europe%27s%20%E2%80%9CDigital%20Decade%E2%80%9D> accessed March 13 2021

EC, 'Foreign Policy' (*EC*, 2021) <https://digital-strategy.ec.europa.eu/en/policies/foreign-policy> accessed February 28 2021

EC, 'The Digital Services Act: ensuring a safe and accountable online environment' (*EC*, 2020) (A safe and accountable online environment) <https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en> accessed March 16 2021

EP, 'Digital Services Act: Legislative train schedule' (*EP*, 2021) <https://www.europarl.europa.eu/legislative-train/api/stages/report/current/theme/a-europe-fit-for-the-digital-age/file/digital-services-act> accessed March 15 2021

EC, 'The Digital Markets Act: ensuring fair and open digital markets' (2020) <https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en> accessed March 24 2021

EC, 'The Digital Services Act package' (2021) <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package> accessed March 22 2021

EC, 'Data policies and legislation - 'Timeline' (2020) <https://ec.europa.eu/digital-single-market/en/data-policies-and-legislation-timeline> accessed March 28 2021

EDPS, 'Shaping a Safer Digital Future: a New Strategy for a New Decade' (2021) <https://edps.europa.eu/press-publications/publications/strategy/shaping-safer-digital-future_en> accessed March 30 2021

EC, 'Measuring Digital Skills across the EU: EU wide indicators of Digital Competence' (2014) <https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=5406> accessed April 2021

EC, 'Digital Education Action Plan (2021-2027)' (2020) <https://ec.europa.eu/education/sites/default/files/document-library-docs/deap-communication-sept2020_en.pdf> accessed March 29 2021

EC, 'Europe fit for the Digital Age: New online rules for businesses'<https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment/europe-fit-digital-age-new-online-rules-businesses_en> accessed March 25 2021

YourEurope, Data protection and online privacy (*EC*, 2021)

EDPS, 'Mobile devices' <https://edps.europa.eu/data-protection/data-protection/reference-library/mobile-devices_en> accessed April 17 2021.

EC, ‘How the IPCR crisis response mechanism works’ (*EU*, 2020) <https://www.consilium.europa.eu/en/infographics/ipcr-mechanism/#:~:text=Text%20version,complex%20crisis%2C%20including%20terrorist%20acts> accessed April 22 2021

EC, ‘Timeline COVID-19 coronavirus’ (*EU*, 2021) <https://www.consilium.europa.eu/en/policies/coronavirus/timeline/> accessed May 1 2021

EC, ‘Digital technologies - actions in response to coronavirus pandemic’ (2020) <https://ec.europa.eu/digital-single-market/en/content/digital-technologies-actions-response-coronavirus-pandemic-online-platforms-and> accessed January 28 2021

EC, ‘Shaping Europe’s digital future: Digital Single Market’ <https://ec.europa.eu/digital-single-market/en> accessed May 9 2021

EC, ‘Digital solutions during the pandemic’ <https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/digital-solutions-during-pandemic_en> accessed May 3 2021

EC, ‘Exchange of electronic health records across the EU’ <https://digital-strategy.ec.europa.eu/en/policies/electronic-health-records> accessed May 2 2021

EC, ‘A Digital Single Market for the benefit of all Europeans’ [2019] <https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53056> accessed May 7 2021

Wiewiórowski W, ‘COVID-19’ (EDPS, 2020) <https://edps.europa.eu/data-protection/our-work/subjects/covid-19_en> accessed April 29 2021

# SUPPLEMENTARY

A4L, ‘Student Privacy and COVID-19’ [2020] <https://cdn.ymaws.com/www.a4l.org/resource/resmgr/docs/whitepaper/student_privacy_and_covid-19.pdf> accessed April 21 2021

Association for Progressive Communications (APC), ‘The EU's plans for its digital future’ (*Apc News*, 2020) <https://www.apc.org/en/news/eus-plans-its-digital-future> accessed March 13 2021

Authenticity Consulting, ‘What is a System?’ LLC <https://managementhelp.org/systems/defn-system.pdf> accessed April 17 2021

BC, ‘Covid: How are European countries tackling the pandemic?’ (2020) <https://www.bbc.com/news/explainers-53640249> accessed April 30 2021

Beaubin J, ‘More Companies Are Using Technology To Monitor For Coronavirus In The Workplace’ (*NPR*, 2020) <https://www.npr.org/2020/10/13/918315238/more-companies-are-using-technology-to-monitor-for-coronavirus-in-the-workplace?t=1619293477836> accessed April 27 2021

Bender D, ‘GDPR harmonization: Reality or myth?’ (*IAPP,* 2018) <https://iapp.org/news/a/gdpr-harmonization-reality-or-myth/> accessed February 8 2021

Bird&Bird, ‘CJEU decision on dynamic IP addresses touches fundamental DP law questions’ (*B&B* 2016) <https://www.twobirds.com/en/news/articles/2016/global/cjeu-decision-on-dynamic-ip-addresses-touches-fundamental-dp-law-questions> accessed February 22 2021

Blankertz A and Jaursch B, ‘How the EU plans to rewrite the rules for the internet’ (*Brookings*, 2020) <https://www.brookings.edu/techstream/how-the-eu-plans-to-rewrite-the-rules-for-the-internet/> accessed March 11 2021

Blankertz A and Jaursch J, ‘What the European DSA and DMA proposals mean for online platforms’ (*Brookings*, 2021) <https://www.brookings.edu/techstream/what-the-european-dsa-and-dma-proposals-mean-for-online-platforms/> accessed March 11 2021

Bloomberg J, ‘Digitization, Digitalization, And Digital Transformation: Confuse Them At Your Peril’ (*Forbes*, 2018) <https://www.forbes.com/sites/jasonbloomberg/2018/04/29/digitization-digitalization-and-digital-transformation-confuse-them-at-your-peril/>

Bräutigam T, ’CJEU Fashion ID Case: Thumbs down to Facebook's’ (B&B, 2019) <https://www.twobirds.com/en/news/articles/2019/global/cjeu-fashion-id-case-thumbs-down-to-facebook%27s-like-feature> accessed March 4 2021

Brown A, ‘Impact on data processors’ (*Simmons & Simmons*) <https://www.simmons-simmons.com/en/features/european-data-protection-regulation/ck0zgbujqdfiu0b49om90f11g/european-data-protection-regulation-impact-on-data-processors> accessed February 26 2021

Burwell F, ‘First privacy, now data: The EU seeks a managed digital space’ (*Atlantic Council*, 2020) <https://www.atlanticcouncil.org/blogs/new-atlanticist/first-privacy-now-data-the-eu-seeks-a-managed-digital-space/> accessed March 6 2021.

Bussche A and Voigt P, ‘GDPR Processor Obligations’ (*Taylor Wessing*, 2020) <https://www.taylorwessing.com/en/insights-and-events/insights/2020/08/gdpr-processor-obligations> accessed March 2 2021

Busse C and Others, ‘The crisis that made the European Union: European cohesion in the age of covid’ (ECFR, 2020)<https://ecfr.eu/publication/the-crisis-that-made-the-european-union-european-cohesion-in-the-age-of-covid/> accessed May 1 2021

Caballero-Anthony M, ‘COVID-19 in Southeast Asia’ (*Brookings*, 2020) <https://www.brookings.edu/blog/order-from-chaos/2021/01/14/covid-19-in-southeast-asia-regional-pandemic-preparedness-matters/> accessed April 22 2021

CDC, ‘Contact Tracing: Using Digital Tools and Monitoring the Disease’ (2019) <https://www.cdc.gov/coronavirus/2019-ncov/cases-updates/about-epidemiology/monitoring-and-tracking.htm> accessed May 7 2021

COE, ‘COVID-19 and Data Protection’ <https://www.coe.int/en/web/data-protection/covid-19-data-protection> accessed May 5 2021

Cory N and Others, ‘Schrems II’: What Invalidating the EU-U.S. Privacy Shield Means for Transatlantic Trade and Innovation’ (*ITIF*, 2020) <https://itif.org/publications/2020/12/03/schrems-ii-what-invalidating-eu-us-privacy-shield-means-transatlantic> accessed March 28 2021

Cox D, ‘The rise of employee health tracking’ (*BBC*, 2020) <https://www.bbc.com/worklife/article/20201110-the-rise-of-employee-health-tracking> accessed April 28 2021

Crowley D, ‘Data Processing at Work: The Right to Rectification and Erasure’ (*Legal Island*, 2018) <https://www.legal-island.ie/articles/ire/features/hot-topics/2018/jan/data-processing-at-work-right-to-rectification-and-erasure/> accessed February 18 2021

CWB, ‘Balancing Employee Privacy and Protection’ <https://www.corporatewellnessmagazine.com/article/covid-19-balancing-employee-privacy-and-protection> accessed May 8 2021

Dataguise, ‘Data Accuracy: GDPR Principles of Processing’ (GDPR Knowledge Center) <https://www.dataguise.com/gdpr-knowledge-center/data-accuracy/> accessed February 13 2021

De la Torre L F, ‘Valid purposes for processing (‘lawful basis’) under EU data protection law’ (*Medium Golden Data*, 2019) <https://medium.com/golden-data/valid-purposes-for-processing-under-eu-data-protection-law-3c1fd9f4b925> accessed February 23 2021

De la Torre L F, ‘Right to rectification under EU data protection law’ (*Medium Golden Data*, 2019) <https://medium.com/golden-data/right-to-rectification-35ec099df2fc> accessed February 13 2021

De la Torre L F, ‘What does “accuracy” mean under EU Data Protection law?’ (*Medium Golden Data*, 2019) <https://medium.com/golden-data/what-does-accuracy-mean-under-eu-data-protection-law-dbb438fc8e95> accessed February 14 2021

Dyani Lewis, ‘Contact-tracing apps help reduce COVID infections, data suggest’ (*Nature*, 2021) <https://www-nature-com.db.ub.oru.se/articles/d41586-021-00451-y> accessed May 4 2021

EPIC, ‘Max Schrems v. Data Protection Commissioner’ (*Epic.Org*) <https://epic.org/privacy/intl/schrems/> accessed March 20 2021

EPIC, ‘Search Engine Privacy’ (2016) <https://epic.org/privacy/search-engine/> accessed April 4 2021

EpiServer, ‘COVID-19’s impact on data privacy, protection and security’ <https://www.episerver.com/guides/covid-19-privacy-considerations> accessed May 7 2021

Eustice J, ‘Understanding data privacy and cloud computing’ (*Thomson Reuters*) <https://legal.thomsonreuters.com/en/insights/articles/understanding-data-privacy-and-cloud-computing> accessed April 4 2021

Finn R, ‘The right to rectification – clarifications from the Data Protection Commission’ (*Trilateral Research*) <https://www.trilateralresearch.com/the-right-to-rectification-clarifications-from-the-data-protection-commission/#:~:text=According%20to%20Article%2016%20of,it%20is%20inaccurate%20or%20incomplete> accessed February 15 2021

Fogarty P and Others, ‘Coronavirus: How can society thrive post-pandemic?’ (*BBC*, 2020) <https://www.bbc.com/worklife/article/20201021-coronavirus-the-possible-long-term-mental-health-impacts> accessed February 3 2021

Frakenfield, J ‘Cloud Computing’ (*Investopedia*, 2020) <https://www.investopedia.com/terms/c/cloud-computing.asp#:~:text=Key%20Takeaways-,Cloud%20computing%20is%20the%20delivery%20of%20different%20services%20through%20the,and%20retrieve%20them%20on%20demand> accessed April 10 2021

Fukuyama F, ‘The Thing That Determines a Country’s Resistance to the Coronavirus’ (*Atlantic*, 2020) <https://www.theatlantic.com/ideas/archive/2020/03/thing-determines-how-well-countries-respond-coronavirus/609025/> accessed May 5 2021

GCT, ‘MEP Eva Kaili: Greece Can Become The Next "success Story" Of Europe’ <https://greekcitytimes.com/2020/12/30/kaili-greece-success-story-europe/> accessed May 5 2021

Gerlach N and Others, ‘CJEU Judgment In The Fashion ID Case: The Role As Controller Under EU Data Protection Law Of The Website Operator That Features A Facebook 'Like' Button’ (*Mondaq*, 2019) <https://www.mondaq.com/unitedstates/data-protection/833684/cjeu-judgment-in-the-fashion-id-case-the-role-as-controller-under-eu-data-protection-law-of-the-website-operator-that-features-a-facebook-39like39-button> accessed February 14 2021

Global Freedom of Expression, ‘GC, AF, BH, ED v. National Commission on Informatics and Liberty (CNIL)’ (GFE) <https://globalfreedomofexpression.columbia.edu/cases/gc-v-national-commission-on-informatics-and-liberty-cnil/> accessed February 18 2021

Global Freedom of Expression, ‘Schrems v. Data Protection Commissioner’ (*GFE Columbia University*, 2020) <https://globalfreedomofexpression.columbia.edu/cases/schrems-v-data-protection-commissioner/> accessed March 23 2021

Greenpeace, ‘How the EU's response to the Covid-19 pandemic could make our society more resilient’ *GEU*, 2020) <https://www.greenpeace.org/eu-unit/issues/democracy-europe/2673/how-the-eus-response-to-the-covid-19-pandemic-could-make-our-society-more-resilient/> accessed April 22 2021

Gustas M, ‘Empowering Community Engagement with the EU's General Data Protection Regulation’ (*SPP*, 2018) <https://www.socialpinpoint.com/blog/empowering-community-engagement-with-the-eus-general-data-protection-regulation/#comments> accessed February 11 2021

Guterres A, ‘Remarks to Member States on Priorities for 2021’ (*UN*, 2020) <https://www.un.org/sg/en/content/sg/speeches/2021-01-28/remarks-member-states-priorities-for-2021> accessed May 9 2021

Hackmann J, ‘How digitalization is changing the demand for software’ (*Sitsi*, 2019) <https://www.sitsi.com/how-digitalization-

changing-demand-software-development> accessed April 18 2021

Håkansson M, 'GDPR: A Driver for Digitalization' (*Axiomatics*, 2017) <https://www.axiomatics.com/blog/gdpr-driver-digitalization/> accessed January 24 2021

Harwell D, 'Mass school closures in the wake of the coronavirus are driving a new wave of student surveillance' (*TWP*, 2020) <https://www.researchgate.net/publication/347933515_Need_for_faster_response_of_education_and_research_system_to_covid_-19_English_version> accessed May 8 2021

Harwood S, 'Data protection and coronavirus' (2020) <https://www.shlegal.com/news/data-protection-and-coronavirus-what-you-need-to-know> accessed May 3 2021

Hatzigeorgiou M and Raj M, 'Why is Greece an outlier in EU's Covid-19 response?' (*EUObserver*, 2020) <https://euobserver.com/opinion/148397> accessed May 4 2021

Hatzopoulos V, 'Taming the COVID-19, not the GDPR: the case of Greece' (*BlogDroitEuropeen*, 2020) <https://blogdroiteuropeen.com/2020/07/04/taming-the-covid-19-not-the-gdpr-the-case-of-greece-by-vassilis-hatzopoulos/> accessed May 5 2021

Heywood D, 'Obligations on data processors under the GDPR' (*GDH*, 2016) <https://globaldatahub.taylorwessing.com/article/obligations-on-data-processors-under-the-gdpr> accessed March 2 2021

HIPAA, 'Upgrading Software to comply with GDPR' (2018) <https://www.hipaajournal.com/upgrading-software-comply-gdpr/> accessed April 18 2021

I-SCOOP, 'Data subject rights under GDPR - the fundamental and contextual rights' (*IS EU*) <https://www.i-scoop.eu/gdpr/data-subject-rights-gdpr/> accessed February 9 2021

I-SCOOP, 'What is a data processor and what are the duties of a data processor under the GDPR?' <https://www.i-scoop.eu/gdpr/data-processor-gdpr/> accessed March 2 2021

IApp, 'CJEU releases judgement on Fashion ID' (*IAPP*, 2019) <https://iapp.org/news/a/cjeu-rules-websites-responsible-for-data-processing-via-facebook-like-button/> accessed March 3 2021

ICO, 'Data protection and coronavirus - what you need to know' (*ICO*) <https://ico.org.uk/global/data-protection-and-coronavirus-information-hub/data-protection-and-coronavirus/> accessed January 30 2021

IISD, 'UN Secretary-General Presents 10 Priorities for 2021 Knowledge Hub' (*SDGKH,* 2021) <https://sdg.iisd.org/news/un-secretary-general-presents-10-priorities-for-2021/> accessed May 9 2021

Illing S and Brookes M, 'The European Commission reports after two years of the GDPR' (*Lewis Silkin*, 2020) <https://www.lewissilkin.com/en/insights/the-european-commission-reports-after-two-years-of-the-gdpr> accessed May 2 2021

IMY, 'Data controllers and data processors' <https://www.imy.se/other-lang/in-english/the-general-data-protection-regulation-gdpr/data-controllers-and-data-processors/> accessed February 23 2021

IMY, 'Lawful grounds for personal data processing' <https://www.imy.se/other-lang/in-english/the-general-data-protection-regulation-gdpr/lawful-grounds-for-personal-data-processing/> accessed February 12 2021

Joyce j, 'Sharing personal data in the context of COVID-19' (*GDH*, 2020) <https://globaldatahub.taylorwessing.com/article/sharing-personal-data-in-the-context-of-covid-19> accessed May 6 2021

Kannengeiser E and Fleck J, 'Europe's new legislative proposals mark a big 'first move' on tech-market power' (*Atlantic Council*, 2020) <https://www.atlanticcouncil.org/blogs/new-atlanticist/europes-new-legislative-proposals-mark-a-big-first-move-on-tech-market-power/> accessed March 18 2021

Kelion l, 'Google wins landmark right to be forgotten case' (BBC News, 2019) <https://www.bbc.com/news/technology-49808208> accessed February 25 2021.

Kittichaisaree K and Kuner C, 'The Growing Importance of Data Protection in Public

International Law' (*EJIL*, 2015) <https://www.ejiltalk.org/the-growing-importance-of-data-protection-in-public-international-law/> accessed March 4 2021

Kuner C, The Schrems II judgment of the Court of Justice and the future of data transfer regulation (*ELB*, 2020) <https://europeanlawblog.eu/2020/07/17/the-schrems-ii-judgment-of-the-court-of-justice-and-the-future-of-data-transfer-regulation/> accessed March 21 2021

Lambert A, 'Coronavirus and the GDPR – keep calm and carry on?' (*Fieldfisher*, 2020) <https://www.fieldfisher.com/en/services/privacy-security-and-information/privacy-security-and-information-law-blog/coronavirus-and-the-gdpr> accessed Janaury29 2021

Lecher C, 'Schools Are Buying Up Surveillance Technology to Fight COVID-19' (*MarkUp*, 2018) <https://themarkup.org/coronavirus/2020/09/08/school-reopening-surveillance-contact-tracing> accessed May 3 2021

Llanso E, 'The DSA: An Opportunity to Build Human Rights Safeguards into Notice and Action' (*Medium Global Network Initiative* (GNI) 2020)

Lohrmann D, '2020: The Year the COVID-19 Crisis Brought a Cyber Pandemic' (*GovTech*, 2020) <https://www.govtech.com/blogs/lohrmann-on-cybersecurity/2020-the-year-the-covid-19-crisis-brought-a-cyber-pandemic.html#:~:text=One%20specific%20example%20comes%20from,cyberattacks%20in%20late%20April%202020.&text=%22Since%20the%20start%20of%20the,targeting%20the%20public%20at%20large> accessed May 3 2021

Lovells H, 'Coronavirus and data protection – Guidance by data protection authorities' [2020] <https://www.hoganlovells.com/~/media/hogan-lovells/pdf/2020%20PDFs/2020_03_19_Coronavirus_and_data_protection_Guidance_by_DPAs.pdf> accessed May 3 2021

Lovells, H 'Shaping Europe's Digital Future – EU publishes its draft Digital Services Act' (JD Supre, 2020) <https://www.jdsupra.com/legalnews/shaping-europe-s-digital-future-eu-75285/> accessed March 10 2021

Lund University, 'COVID Symptom Tracker app launched in Sweden' (*LU*, 2020) <https://www.lunduniversity.lu.se/article/covid-symptom-tracker-app-launched-sweden> accessed May 5 2021

Maenpaa C, 'The GDPR and 25 May 2018: The finishing-line or starting pistol for data protection compliance?' (*Fleishman Hillard,* 2018) <https://fleishmanhillard.eu/2018/05/the-gdpr-and-25-may-2018-the-finishing-line-or-starting-pistol-for-data-protection-compliance/> accessed February 11 2021

Mahieu R and Hoboken J V, 'Fashion-ID: Introducing a phase-oriented approach to data protection?' (*ELB*, 2019) <https://europeanlawblog.eu/2019/09/30/fashion-id-introducing-a-phase-oriented-approach-to-data-protection/> accessed March 1 2021

Marsiglia M, '3 ways Software Products are Different from Physical Products' (*SAO*, 2014) <https://spin.atomicobject.com/2014/07/31/software-products-vs-physical-products/#:~:text=Unlike%20physical%20products%2C%20software%20products,systems%20or%20web%20browsers%20updates> accessed Aprul 5 2021

Martin N and Shabestari N M, 'The right to be forgotten: the CJEU sides with Google in two landmark cases' (*NRF Blog*, 2019) <https://www.dataprotectionreport.com/2019/10/the-right-to-be-forgotten-the-cjeu-sides-with-google-in-two-landmark-cases/> accessed February 19 2021

Maxmen A, 'Why did the world's pandemic warning system fail when COVID hit?' (*Nature*, 2021) <https://www.nature.com/articles/d41586-021-00162-4> accessed April 20 2021

McGinley M, 'Schrems II Judgement: Standard Contractual Clauses' (*Eversheds Sutherland*, 2020) <https://www.eversheds-sutherland.com/global/en/what/articles/index.page?ArticleID=en/global/ireland/schrems-ii-judgement-170720> accessed March 21 2021

Melo S, 'How your company can benefit from digital transformation' (*DataScope*, 2018) <https://mydatascope.com/blog/en/how-can-your-company-benefit-from-digital-transformation/#:~:text=Business%20digitization

%20reduces%20operating%20costs,business%20models%20and%20revenue%20sources> accessed January 25 2021

Meltzer J P, 'The Court of Justice of the European Union in Schrems II' (*Brookings*, 2020) <https://www.brookings.edu/research/the-court-of-justice-of-the-european-union-in-schrems-ii-the-impact-of-gdpr-on-data-flows-and-national-security/> accessed March 20 2021

Metcalf K N, 'COVID-19: Health or Privacy. Do We Have to Choose?' (*RWI Blog*, 2020) <https://rwi.lu.se/blog/covid-19-health-or-privacy-do-we-have-to-choose/> accessed January 29 2021

Microsoft Azure, 'What Is Cloud Computing? A Beginner's Guide' <https://azure.microsoft.com/en-us/overview/what-is-cloud-computing/> accessed April 6 2021

Miladinovic S, 'Is COVID-19 accelerating digitalisation or exposing the digital divide?' (*NewEurope*, 2020) <https://www.neweurope.eu/article/is-covid-19-accelerating-digitalisation-or-exposing-the-digital-divide/> accessed May 2 2021

Miner L and Others, 'How has the COVID-19 pandemic changed our lives globally?' (*EuroNews*, 2020) <https://www.euronews.com/2020/12/23/how-has-the-covid-19-pandemic-changed-our-lives-globally> accessed April 20 2021

Mitsios S, 'GREECE COVID-19: How should Greek companies respond in compliance with the GDPR?' (*EY*, 2020) <https://www.ey.com/en_gr/tax/tax-alerts/greece-covid-19-how-should-greek-companies-respond-in-compliance-with-the-gdpr> accessed May 7 2021

Molla R, 'People say they care about privacy but they continue to buy devices that can spy on them' (*Vox*, 2019) <https://www.vox.com/recode/2019/5/13/18547235/trust-smart-devices-privacy-security> accessed April 17 2021

Muldrew E, 'Why is there a demand for software product management?' (*Medium*, 2019) <https://edwardmuldrew.medium.com/why-is-there-such-a-demand-for-software-product-management-ffaf04da8731> accessed April 5 2021

Naomi Xu Elegant, 'How countries in Asia kept a handle on COVID-19 outbreaks' (*Fortune*, 2020) <https://fortune.com/2020/12/28/asia-covid-success-stories-lessons-learned/> accessed May 1 2021

Nguyen A, 'On the Clock and at Home: Post-COVID-19 Employee Monitoring in the Workplace' (*SHRM*, 2020) <https://www.shrm.org/executive/resources/people-strategy-journal/summer2020/Pages/feature-nguyen.aspx> accessed April 28 2021

NYT, 'Google Coronavirus Apps Give It Way to Access Location Data' (*New York Times*, 2020) <https://www.nytimes.com/2020/07/20/technology/google-covid-tracker-app.html> accessed May 4 2021

Overly S and Ravindranath M, 'Google and Apple's rules for virus tracking apps sow division among states' (*Politico*, 2020) <https://www.politico.com/news/2020/06/10/google-and-apples-rules-for-virus-tracking-apps-sow-division-among-states-312199> accessed May 8 2021

Oxford, 'COVID-19 Government Response Tracker' <https://www.bsg.ox.ac.uk/research/research-projects/covid-19-government-response-tracker> accessed April 22 2021

Paydos T, 'The essential role of government during COVID-19' (*IBM*, 2020) <https://www.ibm.com/thought-leadership/institute-business-value/blog/covid-19-government> accessed April 21 2021

Peckham B, 'Internet vs telecommunications: difference that matters for users' rights' (*Valicom*, 2019) <https://www.valicomcorp.com/blog/2019/1/28/internet-vs-telecommunication-services-differences-that-matter-for-users-rights#:~:text=The%20internet%20is%20a%20global,and%20data%2C%20using%20electronic%20devices> accessed April 3 2021

Penn M, 'How Some Asian Countries Beat Back COVID-19' (*DGHI*, 2020) <https://globalhealth.duke.edu/news/how-some-asian-countries-beat-back-covid-19> accessed April 23 2021

Persiano G, 'Joint Statement on Contact Tracing represented by scientists and researchers from across the globe' [2019] <https://giuper.github.io/JointStatement.pdf> accessed May 8 2021

PWC, 'Balancing employee privacy and public health and safety' <https://www.pwc.com/us/en/library/covid-19/global-privacy-impact-assessment.html> accessed May 8 2021

Privacy Shield Framework, 'Privacy Shield Program Overview' <https://www.privacyshield.gov/Program-Overview> accessed March 23 2021

Rocha R, 'What countries did right and wrong in responding to the pandemic' (*CBC*, 2020) <https://www.cbc.ca/news/canada/covid-19-coronavirus-pandemic-countries-response-1.5617898> accessed April 23 2020

Rutecka D, 'Schrems II – Follow-up On New Protective Measures For Safe Data Transfers' (*Mondaq*, 2020) <https://www.mondaq.com/data-protection/1012794/schrems-ii-follow-up-on-new-protective-measures-for-safe-data-transfers> accessed March 24 2021

Samonte M, 'Google v CNIL Case C-507/17: The Territorial Scope of the Right to be Forgotten Under EU Law' (*ELB*, 2019) <https://europeanlawblog.eu/2019/10/29/google-v-cnil-case-c-507-17-the-territorial-scope-of-the-right-to-be-forgotten-under-eu-law/> accessed February 9 2021

Sauer L M, 'What Is Coronavirus?' (*John Hopkins Medicine*, 2021) <https://www.hopkinsmedicine.org/health/conditions-and-diseases/coronavirus> accessed Janaury 26 2021

Schwartz M, 'Privacy Regulator Promises 'Flexibility'' (*BIS*, 2020) <https://www.bankinfosecurity.com/gdpr-covid-19-privacy-regulator-promises-flexibility-a-14177> accessed May 2021

Shindler a, 'Protecting Personal Data in a Pandemic: GDPR Meets COVID-19 - Part 2' (*JD Supra, Locke Lord LLP*, 2020) <https://www.jdsupra.com/legalnews/protecting-personal-data-in-a-pandemic-39288/> accessed January 30 2021

Simplify, 'You've put GDPR to bed, then you wake up with Schrems II' (*Simplify*, 2020) https://symplify.com/blog/youve-put-gdpr-to-bed-then-you-wake-up-with-schrems-ii/?utm_campaign=schrems&gclid=CjwKCAiAg8OBBhA8EiwAlKw3kq_XyTlStHyFtxfPHgSpVyuzQ4iZre89vPOu_euvAQvn0hHzyCSH9BoCo6wQAvD_BwE> accessed March 15 2021

Spacey J, 'Systems vs softwares' (*Simplicable*, 2016) <https://simplicable.com/new/systems-vs-software#:~:text=Technically%20speaking%2C%20a%20system%20is,term%20for%20any%20computer%20code> accessed March 29 2021

Squareboat, 'Different Types of Software with Examples' <https://squareboat.com/blog/different-types-of-software-with-examples> accessed April 18 2021

Stassen M and Waem H, 'What we can learn about joint controllership from the CJEU Fashion ID ruling' (*Crowell Moring*, 2019) <https://www.crowelldatalaw.com/2019/08/what-we-can-learn-about-joint-controllership-from-the-cjeu-fashion-id-ruling/#page=1> accessed March 3 2021

Stolton S, 'Digital Brief: Schrems 3? Clearview AI furore, EU facial recognition ban' (EurActiv, 2020) <https://www.euractiv.com/section/digital/news/digital-brief-schrems-3-clearview-ai-furore-eu-facial-recognition-ban/> accessed Maarch 13 2021

TermsFeed, 'GDPR Data Processor Requirements' <https://www.termsfeed.com/blog/gdpr-data-processor-requirements/#Data_Processor_Contracts_Playing_By_The_Rules> accessed February 28 2021

Tewari S, 'Schrems II: A brief history, an analysis and the way forward' (*Inforrm*, 2020) <https://inforrm.org/2020/07/23/schrems-ii-a-brief-history-an-analysis-and-the-way-forward-shreya-tewari/> accessed Maarch 21 2021

The Enterprisers Project, 'What is digital transformation?' (*Red Hat*, 2016)

<https://enterprisersproject.com/what-is-digital-transformation> accessed March 7 2021

The Grow, 'Why Is Data Important for Your Business?' (*TGC,* 2020) <https://www.grow.com/company/about-grow> accessed February 12 2021

Thompson S and Warzel C, 'Smartphones are Spies. Here's Whom They Report to' (*New York Times*, 2019) <https://www.nytimes.com/interactive/2019/12/20/opinion/location-tracking-smartphone-marketing.html> accessed May 4 2021

Tidey A and Others, 'Digital Service Act: EU vows to 'put order into chaos' with tech laws' (*EuroNews*, 2020) <https://www.euronews.com/2020/12/15/digital-services-act-brussels-unveils-landmark-plans-to-regulate-tech-companies> accessed March 16 2021

TrustArc, 'Managing Employee Privacy in the Face of COVID-19' (*TrustArc*, 2020) <https://trustarc.com/blog/2020/03/19/managing-employee-privacy-in-the-face-of-covid-19/> accessed April 27 2020

Turner J L, 'Privacy and Security in the Post-Pandemic World' [2021] 11(115) NLR <https://www.natlawreview.com/article/privacy-vs-security-post-pandemic-world> accessed May 1 2021

Tyler C and Gluckman P, 'Coronavirus: governments knew a pandemic was a threat – here's why they weren't better prepared' (The Conversation, 2020) <https://theconversation.com/coronavirus-governments-knew-a-pandemic-was-a-threat-heres-why-they-werent-better-prepared-136857> accessed April 17 2021

UNISON, 'Monitoring and surveillance workplace policies' [2020] <https://www.unison.org.uk/content/uploads/2020/07/Monitoring-and-surveillance-at-work-1.pdf> accessed May 2 2021

United Nations, 'Digital technologies critical in facing COVID-19 pandemic' (DESA, 2020) <https://www.un.org/fr/desa/digital-technologies-critical-facing-covid-19-pandemic> accessed May 9 2021

Van den Brande B, 'The future Digital Services Act and Digital Markets Act in a nutshell' (*Sirius.Legal*, 2021) <https://siriuslegaladvocaten.be/en/the-future-digital-services-act-and-digital-markets-act/> accessed March 16 2021

Verheyen S, 'Why investing in digital literacy now will secure the future of the EU' (*TPM*, 2020) <https://www.theparliamentmagazine.eu/news/article/why-investing-in-digital-literacy-now-will-secure-the-future-of-the-eu> accessed April 4 2021

Warren T, 'Zoom faces a privacy and security backlash as it surges in popularity' (*The Verg*e, 2020) <https://www.theverge.com/2020/4/1/21202584/zoom-security-privacy-issues-video-conferencing-software-coronavirus-demand-response> accessed April 18 2021

Weisbaum H, 'Are the smart devices in your home spying on you?' (*BBT*, 2019) <https://www.nbcnews.com/better/lifestyle/downside-connected-tech-are-smart-devices-your-home-spying-you-ncna1101906> accessed April 16 2021

Wolford B, 'What is GDPR, the EU's new data protection law?' (*GDPR EU*). <https://gdpr.eu/what-is-gdpr/> accessed January 18 2021

ZOE, 'COVID Symptom Study' <https://covid.joinzoe.com/about> accessed May 4 2021