International Journal of Human and Society (IJHS)

P-ISSN: 2710-4966	E-ISSN: 2710-4958
Vol. 4. No. 03 (Jul-Sep) 2024	Page 691-699

Exploring the Competition Challenges to SMEs within European Union Market after application of General Data Protection Regulation (GDRP)

Elyssa Mathlouthi	University of Dundee, Scotland
Anwaar Rana	Lecturer, University of Management and Technology (UMT), Pakistan
Sundus Rauf **(Corresponding Author)**	Assistant Professor, College of Law, The University of Lahore, Pakistan sundas.rauf@law.uol.edu.pk

Abstract: *Within the European Union, the monetization of data has generated an economy of 300 billion in 2016 and has kept on increasing since then. In 2018 the General Data Protection Regulation (GDPR) has been enforced and is said to have drastically changed the European Union landscape of data protection. The impact of such a regulation on the competition within the European Union market can be analysed by tackling the subject from three different angles: the barrier to entry of SMEs into the market, the balance of interests between consumer welfare and data privacy and finally the GDPR as a controversial regulatory tool for the market. The whole topic was discussed by the researcher in her dissertation for postgraduate degree. This paper has been extracted from the thesis and is focussing on the first aspect of the research where the GDPR appears to be a challenge for the small and medium sized enterprises but not to the extent of being a barrier to entry the market thanks to the flexible and tolerant approach of the European Commission and National Data Authorities. Moreover, this approach allowed raising awareness regarding data privacy both on the companies' side and consumers' side. The transparency brought by the GDPR even generated a competitive asset for companies. As a result, both overlapping notions happen to complement each other. Finally, it is likely, considering the current use of the GDPR by the European Commission, that in the long run the GDPR could be used as one of the factors to analyse and control behaviours on a competitive perspective and therefore helping to regulate the market.*

Keywords: General Data Protection Regulation (GDPR), impact, European Union, market, barrier, challenges, SMEs, data, consumer, privacy

Introduction

The European Union market, just like other great markets in the world, is regulated by Competition law and in the present case, by the European Competition Law. As a consequence, National Competition Authorities (NCAs) and the European Commission (EC) aim to protect the consumer welfare which could be expressed inter alia by the access of a wide range of products and services at different price ranges, as well as protecting the competition itself by ensuring healthy competition and allowing small and medium enterprises (SMEs) to have their place in the market. They also aim to promote economic equity through the redistribution of wealth and the dispersal of economic power and, of course, the respect of the single market.

However, even with the work of the European Commission and National Competition Authorities some external factors can cause a distortion of specific markets within the European Market. For example, if a shortage of the raw materials used to manufacture books happens it is likely that the book market will

suffer from it, as well as the competition. But, such kind of distortions can also happen when a new law or regulation is implemented. Indeed, as Richard Epstein said in his critique of the notion, granting positive rights is "always easy, if not inevitable, to expand the set of rights without adverse social consequences" (Layton & Elaluf-Calderwood, 2019).

With the globalization and new technologies, new economies arise and one of them is the *data economy*. Indeed, the monetization of data created a whole new market that holds a multiplicity of markets within it, such as the online advertisement market or social media market. As an example, in 2016 the European Union data economy was worth nearly 300 billion Euros (European Commission, 2017). Through the collection and aggregation of data and more importantly personal data, companies are able, for example, to create personalized advertisements to raise the sales efficiency. However, via this process rights to privacy and data protection of the consumers have a greater chance to be violated.

In order to understand better those violations of rights, it is important to first establish the distinction between the right to privacy and data protection. The right to privacy is guaranteed by the article 12 of the Universal Declaration of Human Rights (United Nations, 1948) and is considered as a fundamental right in several countries. This right provides that "*no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation*" (United Nations, 1948). However, it is not an absolute right, therefore for public policy's reasons or other important national concerns, this right can be restricted. As compared to data protection, the right to privacy is much broader and can be used in several ways (e.g. right to have a private family life). Data protection covers, as its name indicate, data, but more precisely personal data of a person which covers any "*information relating to an identified or identifiable natural person […] such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*" (EUR-Lex, 2016). Data protection is also not considered as an absolute right. In a nutshell, one can say that privacy is the bigger picture and personal data protection is one part of it.

In the European context, it is important to highlight that "*the economic and social integration resulting from the functioning of the internal market has led to a substantial increase in cross-border flows of personal data*." (EUR-Lex, 2016). With this substantial increase in cross-border flows of personal data we can also observe a substantial increase of the unlawful use or use of personal data without a true informed consent. One can namely think about bounded rationality (Lynskey, 2018). People usually think of the bound (acceptance of privacy policies) on a shorter term only. When a user of a particular website agrees on a privacy policy, he rarely reads them or has a bargaining power. These situations lead to a sort of sense of loss of control and a resignation from data subject to protect their personal data and their privacy.

However, data subjects through association, activists and organizations, are willing to fight to protect their rights. Faced with the awakening of the data subjects in Europe, the European Union in 2016 voted a regulation, the General Data Protection Regulation (GDPR), which came into force in May 2018, in order to regulate the use of personal data, strengthen and harmonize the existing laws on data protection and providing more substantial data protection rights to the consumers.

The GDPR is said to have reshaped significantly the data protection regulatory landscape in the European Union and has empowered consumers (coface, 2018). As a direct result any company, based anywhere in the world, but dealing with European consumers' personal data had to comply with this regulation and restrict the use of those data to the GDPR conditions. Moreover, one of the expected results of this regulation would also be the reduced access of the consumers' personal data for those same companies. As said previously, those very same personal data and the use of them by the companies are part of economic models,

especially for e-companies. One might expect therefore an impact on competition law and on the consumers.

The GDPR: A barrier to enter the European Market?

As mentioned earlier, the data market is a growing market in the European Union. However, part of that data is personal data. Personal data, especially if we take in broader definition given by the article 4 of GDPR, allows inter alia to create personalized add and targets more easily the customers by crossing personal data and big data. Big data refers as to *"high-volume, high-velocity and high-variety information assets that demand cost-effective, innovative forms of information processing for enhanced insight and decision making"* (Denham, 2017). The other issue with personal data is the way that some companies process them. Personal data and big data are often mixed and processed in the same way. Therefore, in theory the new regulation of personal data should have an impact on Competition law and on the data economy which mixes big data and personal data. But this impact can happen in two ways: as an external and as an internal constraint.

This research is intended to analyse personal data protection as an internal constraint. Data is at the core of the market, and this new "heavy" regulation which is the GDPR can represent a challenge for companies. However, the application of the GDPR is intended to be flexible and more focused on bigger breaches.

GDPR's Challenges for Companies

Prior to diving into analysing the challenges that companies can face with the GDPR it is important to establish which type of company that we are talking about. The notion of "barrier to entry into the market" could be summarized as *"a factor that makes entry [a market] unprofitable while permitting established firms to set prices above marginal cost, and to persistently earn monopoly return*" (McAfee, Mialon, & Williams, 2004). Therefore, companies that are likely to be prevented to entry a specific market are small and medium-sized enterprises, which we will refer as to SMEs. Indeed, by nature small and medium-sized enterprises are not established or more precisely well established in the market and have low resources which do not allow them to overcome some challenges that can become barriers to entry the market.

One can think about four main challenges for SMEs when it comes to the GDPR. Those challenges are namely the security challenge, that comes along with the cost of compliance, which could be designated, as the economic challenge, data portability and finally the challenge of accessing data.

1. **Security Challenge**

The GDPR provides 8 individual rights to consumers/data subject. Amongst those rights we can find the right to data portability, the right to access data, the right to rectification, the right to erasure and the right of restriction of processing (GDPR, Art 16-20). If a company or an organization is failing to comply properly with the GDPR, the article 83(5) states that administrative fines up to 20 million Euros or, in case of an undertaking, up to 4 percent of the total worldwide annual turnover of the preceding, could be inflicted.

In order to be able to fulfil all the duties arising from the rights introduced by the GDPR companies have to store the personal data in a way that makes them easily accessible in the event where data subjects wish to erase them, transfer them to another company or get them back. The type of storage that suits the best this need of easily accessible data, would usually be a "pool of data" (Layton & Elaluf-Calderwood, 2019). A pool of data is in few words is a process where data sets coming from different sources are combined and merged into one data file (Roadmap, 2024). However, even though the system of pool of data seems to be the most convenient system when it comes to complying with the GDPR, especially for SMEs, since it requires less efforts and smaller costs, it also creates a big issue. Indeed, data pools create "*a target rich environment for cyber criminals*" (ANA, 2019).

This point leads us to the fact that the GDPR has two main consequences that is *on cyber-security*

and *on the security of personal data.*

The first one, which was not expected, is that the threat of substantial fines for non-compliance and the blurry edges of the GDPR has hindered the fight against cyber-criminality, especially in the domain of online identity theft. Indeed, organization such as the Internet Corporation for Assigned Names and Numbers (ICANN) , which manage "Who is responsible for this domain" have chosen to mask personal data in order to prevent any breach to the GDPR, and therefore avoid any substantial fine that could be inflicted, even though the GDPR does not actually require such actions. Therefore, the GDPR has indirectly undermined "the transparency of international systems and architectures that organizes the internet" (ANA, 2019). This problem also shows a lack of clarity on certain aspects of the GDPR. Indeed, even if in its report of 2020 the European Commission did not mention potential amendments to make the GDPR more understandable some associations of data protection officers deplore this (European Commission, 2020).

The second is that due to this resurgence of possible cyber-attacks, companies have to invest in cyber-security in order to fulfil their duties. However, SMEs usually do not have the sufficient budget to have an efficient system of personal data protection, although this is one of the big requirements of the GDPR. Article 32 of the GDPR on "Security of processing" states that' "*the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk*" (GDPR, Art 32). The complexity and the costs generated by the compliance to the GDPR have led some SMEs to decide not to comply with the GDPR, some of those companies even state that a full compliance appears to be undoable (ANA, 2019).

Therefore, maintaining a sufficient level of security in order to protect the personal data, without over doing it, appears to be a true challenge that some SMEs are not willing to take yet. This could have a major impact and represent a barrier to entry to the market considering the substantial fines given by the European Commission and national data authorities.

2. Costs of Compliance

But above this challenge, that securing the processing of personal data represents, the biggest drawback is the cost that represents the compliance to the GDPR, especially for SMEs. In order to anticipate and calculate the risk and cost for the infringement of data protection different methods exist. One of those methods would be the Gordon-Loeb model, which is a mathematical and economic model used to predict a firm's optimal investment in information security in order, not to maximize profit, but to minimize loss. "The optimal amount to spend on information security never exceeds 37% of the expected loss resulting from a security breach (and is typically much less that 37%)" (ENISA, 2012). This shows, how big this could be for SMEs to fully comply and explain why some of them sound reluctant to implement all of the GDPR requirements.

3. Data Portability Challenge

On top of those challenges mentioned, companies have to face another challenge which is Data Portability. Data Portability is definitely one of the rights provided by the GDPR which has been the most talked about because of its newness and its difficulties to be implemented. Article 20 of the GDPR introduces this right which could be explained as the right for the data subject to require from a data controller (generally a company) to hand over the personal data provided by the data subject himself/herself to another data controller in a usable and transferable format or to obtain a copy of those personal data (Vanberg & Unver, 2017).

The problem that seems to stand out the most with data portability is the disproportionate costs and efforts that need to be implemented by the SMEs in order for them to be able to fulfil their duty. To hand over personal data in a secure way, in order to avoid any breach of the GDPR and the heavy fines, companies have to write specialized code: export-import module (EIM). However, it has been found that most SMEs do not have the resources to write an EIM, which can put them at fault (Swire & Lagos, 2013).

Also, data portability could have a detrimental impact on trade secrets and intellectual property. Indeed, in their paper professors Vanberg and Ünver illustrate this through the *True Fit case.*

True fit is an online platform that helps customers to find their "true fit" and true size of clothing and shoe wear amongst the different popular retail brands through the use of personal data. In this case personal data are at the core of the activity of such a company and handing over those data which are essential in the business model would inevitably make the company obsolete. On the long run, the use of data portability could have as a result to deter market players to implement this kind of services and create companies with a business model based practically solely on personal data.

Article 20 of the GDPR also lacks clarity. Indeed, data portability has some limits such as *"technical feasibility"* or the right to privacy of a third party. Those limits are not clearly defined and could help SMEs to lessen the disproportionate costs and efforts, but also it could drastically lessen the collaboration between the market players. But it is important to highlight that, the collaboration between those actors is an important factor that helps elaborate industry standards, especially needed with a new regulation such as the GDPR.

Indeed, some data controller could refuse on the basis of technical feasibility or on the basis that those data involve a third party, and through this block abusively the access of personal data which could be at core of the activity of a company. Data portability leads us to our final point, the access to data.

4. Access to Data

Part of the new obligations for data processors is the fact that in order to process personal data they have to obtain first the informed consent of the data subject and be able to demonstrate it notably by informing data subjects on how those data are going to be used. The GDPR also allows data subjects to withdraw their consent on the use of their personal data at any time, which empowers the data subject but also creates uncertainty for the companies that base their business model on personal data (GDPR, Art 7).

Also the threat of the heavy fines given in case of breach of the GDPR, let it be about security or compliance of other duties, have a deterring effect for companies and might push some of the SMEs that are not able to comply or fully comply to not process personal data at all or at the very minimal (e.g. only processing their employees' personal data for technical support reasons).

All of the duties and the uncertainty created by some rights for the data subjects (withdrawal of their consent, data portability, etc.), lead to difficulties for companies to have access to personal data. This difficulty is not necessarily bad since it allows personal data not to be overused or processed carelessly but one of the side effects is that SMEs especially start-ups will have more difficulties to obtain data and use them since they don't have the same resources that the market champions have and which would allow them in obtain and process those data lawfully. Therefore, it is likely that the already existing big gap between SMEs and big companies such as Google or Facebook, regarding the collection of personal data, will expand, creating or enhancing a barrier to entry the market.

Moreover, since the GDPR is pretty recent, the European Market is not fully harmonized yet in terms of data protection. Some countries like Germany or France had already existing national laws that were pretty protectors for data subjects, which gives a competitive advantage since the gap in order to comply with the GDPR will be smaller than in other countries.

Also, the lack of clarity of some articles of the GDPR can create confusion. This lack of clarity is not only a problem regarding compliance but also creates slight differences between nationals' authorities in charge of the enforcement of the GDPR and which can give different guidelines and threshold (e.g. very low threshold in Germany to mandatorily appoint a DPO).

All of those challenges combined can definitely create a barrier to entry the market for SMEs which are not as well-armed as the big companies which have the means to comply and

which are already settled in the market.

Flexible Application of GDPR

On paper, all those challenges seem to be a big barrier to access the market. However, in practice, things might be a little different. Although, the application of the GDPR is effective as we can see through websites that tracks the substantial fines that are given as a result of the breach of the GDPR (enforcementtracker, 2024) and lately through the striking example of the 50 million Euros fine given to Goggle and confirmed by the Conseil d'État on the 19th of June 2020 (Conseil d'Etat, 2020), SMEs seem to be out of the radar of the European Commission and national data protection authorities. The application of the GDPR is intended to be flexible as we can tell through the guidelines of the CNIL (the French data protection authority) that states that "*the GDPR approach is based on the concept of risk management, thus providing flexibility in defining tailor-made solutions*" (Hamiche, 2018).

This statement translates the European flexible approach and desire of harmonization on the personal data protection field. It seems that the true targets of such drastic measures regarding personal data are big companies that process data on a large scale. Regarding the SMEs national authorities seem to usually be more flexible to evaluate their degree of compliance. Numerous workshops and guidelines, with special mention for SMEs can be found on every website of each European national authority in charge of enforcement of the GDPR (ico, 2024).

It appears pretty clear that the European Commission and national authorities are well aware of the difficulties that represent the compliance with the GDPR and are willing to let companies grow into it with tolerance. This way of approaching the application of the GDPR, by letting more time to SMEs to be able to comply and to change their way of processing personal data appears to be working because we can observe a general awareness regarding that matter.

Companies even go further than this and have found a competitive advantage in the compliance with the GDPR (Le Clerc, 2020). Indeed, the empowerment of consumers and their awareness, have led to another side effect. Transparency regarding process of personal data, brought by the GDPR appeals data subjects which are more willing to report the companies which do not respect their rights. This very same transparency generates this competitive asset found by some companies. Companies have found that they are able to develop a trust relationship with the consumers through the compliance of the GDPR and through the transparency of the use of the consumers' personal data. As a result, consumers are more willing to give their data and personal data, which gives an advantage over less conscientious companies within the data economy, where the market power is partly established through the collection of data.

Moreover, the GDPR works with a "one-stop-shop" system (Lopes, Guarda, & Oliveira, 2019). This one-stop-shop system allows companies to have contact with only one national authority even when they are processing personal data of consumers coming from different European countries. The one stop-shop has two side effects: allowing more clarity because companies have to address and follow only the national authority of the country where they have their headquarter and lessen the effects of the slight differences between the different national authorities.

Also, as we said before, the GDPR empowers a lot the consumers. They are encouraged to use their rights by reporting to national authorities the breaches made to the GDPR. However, it is more likely that they will report big companies that are in their day-to-day lives such as Google or Facebook, than SMEs which they will have only a few exchanges on the occasion of the use of their services. The fact also that those companies are SMEs and that they are not fully settled into the market lessen the chances of breach considering that they will process fewer personal data than the giants on the European data or personal data market.

It is also important to highlight that SMEs depending on their size and activities will have less cost than bigger companies. Indeed, it will

depend on companies' hard or soft assets. A company that will process less data or process data indirectly, will have as a consequence less cost of investment in cyber security. Those SMEs will also have fewer obligations than bigger companies, for example, some requirements like the Data Protection officer (DPO), which is a key officer in the implementation of the GDPR, and which is translated by the need of hiring a DPO or to carry out training of a company member which will generate costs for the company are not mandatory for every company. Article 37(1) of the GDPR states that designating a Data Protection Officer is mandatory only in three cases even if it is still recommended for other companies. The three mandatory cases are the following:

"(a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;

(b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or

(c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10. "

The expression used "*large scale"* could lack of clarity for many companies, however, the European Commission released guidelines on data protection officer in order to explain better this key role (European Commission, 2017). National authorities also provide information on that matter (ICO, 2022), which leads to believe that most SMEs will not have to designate a DPO if they do not wish to.

Regarding the challenge created by data portability, we can observe two points. The first point would be the limitation of the scope of data portability by the privacy rights of third parties. This limitation is likely to discourage the data subject to use data portability because data processors will be able to decline their requests on that basis. The second point, is that article 15 of the GDPR "right of access of the data subject" is limited in its scope by the recital 63. This recital provides that if this right adversely affects the rights and freedoms of others, including trade secrets and intellectual property rights, it will be restricted. Even though data portability has not the same limitation and that the European Commission has not mentioned an intention to modify or clarify aspects of the GDPR in its last report, it is likely that if data portability encounter too many difficulties to be implemented by the companies or has a negative effect on the competition market, a similar scope will be set.

Finally, the GDPR encourages the use of a system of information security management which can help and provide many advantages to companies such as "reducing the costs associated with 'non-security'. One of the examples of those systems is the ISO 27001 standard which is an international framework for information security management. This system provides a solid ground for companies in terms of personal data protection, doing most of the work for them. However, there is still a need to go further in order to adjust to the GDPR requirements but as the application of the GDPR is meant to be in a flexible way, this kind of system are great first steps to comply more easily. More collaborative solutions like initiative CRM, which is a customer relationship management software, exist, enabling SMEs to gain precious time (Decideo, 2019).

Conclusion

In order to summarize this, at first glance the GDPR appears to be a barrier to entry the market for SMEs. However, even if the compliance is not easy, companies are really willing to work on it and are becoming aware of the importance of personal data protection, including through the aspect of competitive advantage. The European Commission and national authorities are also choosing to implement this recent regulation in order to facilitate its entrance in the European legal landscape. As a result, the GDPR seems not to be a hermetic barrier to entry the market and have a surprising side effect,

including the awakening of most of the consumers of the EU. In a nutshell, the GDPR has an internal and external constraint on the European Market. From the internal point of view, it had an impact on the competitors because of the challenges that it brings, and the substantial fines implemented. But overall, the main target is big companies which allow maintaining healthy competition and serving the interests of the consumers. And finally, from the external point of view, used under conditions, it could act as a very relevant tool to control the competition.

References

ANA. (2019, March 4). *The CCPA---Making things worse*. Retrieved from https://www.ana.net/blogs/show/id/rr-blog-2019-01-The-CCPA-Making-Things-Worse

coface. (2018). *Personal Data Protection*. Retrieved from https://www.coface.com/personal-data-protection

Conseil d'Etat. (2020, June 19). *GDPR: Council of State rejects appeal against 50 million euro fine imposed on Google by CNIL*. Retrieved from https://www.conseil-etat.fr/actualites/rgpd-le-conseil-d-etat-rejette-le-recours-dirige-contre-la-sanction-de-50-millions-d-euros-infligee-a-google-par-la-cnil

Decideo. (2019, July 23). *GDPR: VSEs/SMEs are lagging behind... but not for long*. Retrieved from https://www.decideo.fr/RGPD-Les-TPE-PME-a-la-traine-mais-plus-pour-longtemps_a11248.html

Denham, E. (2017, September 4). *Big data, artificial intelligence, machine learning and data protection.* Retrieved from Information Commissioner's Office (ICO): https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf

enforcementtracker. (2024). *GDPR Enforcement Tracker*. Retrieved from https://www.enforcementtracker.com/

ENISA. (2012). *Introduction to return on security, Helping CERTs assessing the cost of (lack of) security"* . Retrieved from https://www.enisa.europa.eu/publications/introduction-to-return-on-security-investment/@@download/fullReport

EUR-Lex. (2016, December 16). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Da*. Retrieved from https://eur-lex.europa.eu/eli/reg/2016/679/oj

European Commission. (2020, June 24). *Commission report: EU data protection rules empower citizens and are fit for the digital age*. Retrieved from https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1163

European Commission. (2017, October 30). *Guidelines on Data Protection Officers ('DPOs') (wp243rev.01)*. Retrieved from https://ec.europa.eu/newsroom/article29/items/612048

European Commission. (2017, October 30). *Guidelines on Data Protection Officers ('DPOs') (wp243rev.01)*. Retrieved from https://ec.europa.eu/newsroom/article29/items/612048

European Commission. (2017, May 2). *Shaping Europe's digital future:Final results of the 2014-2016 European Data Market study measuring the size and trends of the EU data economy*. Retrieved from https://digital-strategy.ec.europa.eu/en/library/final-results-2014-2016-european-data-market-study-measuring-size-and-trends-eu-data-economy

GDPR. (Art 16-20). General Data Protection Regulations.

GDPR. (Art 32). *General Data Protection Regulations*. Retrieved from https://gdpr-info.eu/art-32-gdpr/

GDPR. (Art 7). *General Data Protection Regulations*.

Hamiche, S. (2018, April 18). *GDPR: A Practical Guide for Small Businesses*. Retrieved from https://www.lemondedesartisans.fr/actualites/rgpd-un-guide-pratique-pour-les-petites-entreprises

ico. (2024). *Data protection in school*. Retrieved from https://ico.org.uk/

ICO. (2022, October 14). *Guide to the General Data Protection Regulation*. Retrieved from Information Commissioner's Office: https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr-1-1.pdf

Layton, R., & Elaluf-Calderwood, S. (2019). A Social Economic Analysis of the Impact of GDPR on Security and Privacy Practices. *12th CMI Conference on Cybersecurity and Privacy (CMI).*

Le Clerc, M. D. (2020, May 13). *EU: GDPR Survey: Benefits beyond compliance*. Retrieved from https://www.globalcompliancenews.com/2020/05/13/eu-gdpr-survey-benefits-beyond-compliance-27042020/

Lopes, I. M., Guarda, T., & Oliveira, P. (2019). How ISO 27001 Can Help Achieve GDPR Compliance. *2019 14th Iberian Conference on Information Systems and Technologies (CISTI).*

Lynskey, O. (2018). *How can privacy and data protection be integrated into competition law? OECD Compitition Division.* Retrieved from https://www.youtube.com/watch?v=bN3m7YBtRJE

McAfee, R. P., Mialon, H. M., & Williams, M. A. (2004). What is a Barrier to Entry? *The American Economic Review , 94* (2), 461-465.

Roadmap. (2024). *What is data pooling?* Retrieved from https://www.roadmap-alzheimer.org/faq/what-is-data-pooling/

Swire, P., & Lagos, Y. (2013). Why the right to Data Portability likely reduces consumer welfare: Antitrust and privacy critique. *Maryland Land Review , 72* (2).

United Nations. (1948). *General Assembly Resolution 217 A: Universal Declaration of Human Rights 1948*. Retrieved from https://www.un.org/en/about-us/universal-declaration-of-human-rights

Vanberg, A. D., & Unver, M. B. (2017). The right to data portability in the GDPR and EU competition law: odd couple or dynamic duo? *Bileta Special Issues-Future, Law, Education and Technology , 8* (1).