How Does Data Portability Affect M&A? An Operationalization Analysis Through M&A Phases

Gabriel Araújo Souto

1. Introduction

Data portability is the possibility of transferring personal data to different platforms. This possibility, enforced by the right to data portability, aims to protect the data storage of users against the incompatibility of multiple platforms, that is, allowing interoperability between different services. Data portability allows, for example, an Instagram user to transfer their data, such as photos and videos, directly to a competitor such as Pinterest, with no barriers to compatibility and preserving the personal data's integrity.

The imposition of data portability would require a certain level of interoperability between platforms. This would benefit both unilateral and multilateral market platforms, as the flow of users would enable the network effect to be enhanced, even more with the practice of multihoming, as well as consumers by mitigating switching costs and lock-in effect.

---

1 Gabriel Araújo Souto is an ambassador of the American Bar Association Section of Antitrust Law's Law Student Ambassador Program.
3 The General Data Protection Regulation (GDPR) introduces the right to data portability, giving individuals greater control over their data. See Publications Office of the European Union. Article 20 of the Regulation (EU) 2016/679 (General Data Protection Regulation) (2016). Luxembourg. The right to data portability not only serves a data protection purpose but also mitigates competing access issues by reducing switching costs and lock-in effect. In the Brazilian context, the Brazilian General Data Protection Law (LGPD) also standardizes the right to data portability. See Diário Oficial da União. Article 18 item V of the Law no. 13.709 (Lei Geral de Proteção de Dados) (2018). Brazil.
6 See Carl Shapiro & Hal R. Varian, Information Rules: A Strategic Guide to the Network Economy, Harvard Business School Press 11-13 (1999) (explaining that the lock-in effect occurs when the consumer, dependent on the infrastructure or a particular service of a company, cannot switch to a competitor without substantial costs or material losses. In this sense, the absence of data portability has the potential to produce this effect to the consumer, since the latter may not be able to transfer its data to another platform, causing the user to remain using the service).
establish an effective form of data portability, technical measures should be in place to easily transfer user data from one platform to another. To some extent, this would require a standard data storage format, such as Application Programming Interfaces (APIs), and could be developed by consortia or international organizations to allow platforms to exchange and use such information mutually.

Indeed, data sharing through APIs or common protocols between purchasers and targets is expected to have a profound market impact in terms of innovation and creation of new market opportunities for various stakeholders, since M&A is already being affected by data protection pressures. These pressures are demonstrated by a 2018 research study by Merrill Corporation analyzing 539 M&A professionals, where 55% of them said they had worked on deals that fell apart because of concerns about a target company’s data protection policies and compliance with GDPR.

Therefore, the implementation of data portability policies and tools by companies prior to M&A operations promotes less costly data transfer between companies and their customers. Furthermore, it increases the efficiency of the operation as the migration of data will be less time consuming, which can mitigate the potential loss of profit by the company’s performance decline when data is critical to its operation. The steps to ensure an effective and compliant M&A operation considering data portability will be noted in the topic below.

2. The Importance and Operationalization of Data Portability in M&A

7 Deloitte, How to Flourish in an Uncertain Future, Open Banking and PSD2, Deloitte LLP Publications 8-9 (2017), https://www2.deloitte.com/content/dam/Deloitte/cz/Documents/financial-services/cz-open-banking-and-psd2.pdf (highlighting open standards of interoperability as important facilitators of competition. For example, the UK antitrust authority, CMA, has demanded Open Banking standards in its attempt to increase competition in the retail banking market by allowing financial technology innovators to enter a market through access to APIs based on common technical standards).
8 See LIMSwiki, Application Programming Interface, LIMSwiki Articles (May 26, 2015), https://www.limswiki.org/index.php/Application_programming_interface (defining API as “a particular set of rules and specifications that software programs can follow to communicate with each other. It serves as an interface between different software programs and facilitates their interaction, similar to the way the user interface facilitates interaction between humans and computers.”).
13 Id.
Personal data is an important aspect of most M&A transactions as almost every company stores information about its employees and customers. Data is critical for some transactions. To explain that, the analysis of the importance of data portability in M&A is structured in the form of a timeline, analyzing each stage of the transaction: (i) pre-signing, (ii) signing, (iii) signing to closing, and (iv) post-closing.

(i) Pre-signing

M&A operations look to combine customer databases to maximize transaction value, but this can raise privacy and data protection compliance issues. The operating efficiencies envisaged for an integrated business may be challenged by cross-border data transfer controls that prevent or restrict consolidation of data center and other operations. Moreover, in a merger setting, remedies of data portability or data sharing may play a role as tools to prevent a merger from significantly impeding effective competition. For example, the European Commission (EC) in the 2008 Thomson/Reuters merger decision, by approving the merger on the condition that the merging parties would divest copies of their databases containing financial information, together with relevant assets, personnel and customer base as appropriate, set a remedy that would allow purchasers of the databases to quickly establish themselves as a relevant competitive force in the market of the merged entity.

14 The importance of data in M&A can be illustrated by the acquisition of Nest by Google in early 2014. See Sophie Curtis, What is Nest and Why Has Google Bought It?, THE DAILY TELEGRAPH (Jan. 14, 2014), https://www.telegraph.co.uk/technology/google/10570414/What-is-Nest-and-why-has-Google-bought-it.html (describing that Nest, a producer of smart home devices such as thermostats and smoke detectors, was not competing with Google in any relevant markets when it was acquired. However, this move by Google has strengthened its position regarding access to data on consumer behavior. The Nest acquisition may have impacted not only Google’s ability to improve the relevance of existing services offered to users and advertisers on its search platform but also enabled Google to develop new products based on new insights gained from data analytics of Nest and by combining it with Google’s information).

15 Hogan Lovells, supra note 5, at 3.

16 See Anca D. Chirita, Data-Driven Mergers under EU Competition Law, The Future of Commercial Law: Ways Forward for Harmonisation 22 (Jul. 13, 2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3199912 (explaining that “[i]n Google/DoubleClick, there were a number of competitive advantages for Google following the integration of DoubleClick’s ad serving technology with ad intermediation services, Double Click’s customer base among publishers and advertisers, and data about consumer behavior collected through ad serving. (…) A portability issue became apparent as advertisers had to transfer ‘past’ data from one system to another. It was, however, estimated that less than 1% of former customers would require the migration of historical delivery data upon switching.”).

Under US law, the pre-closing disclosure of personal data must comply with all relevant state laws, contractual restrictions, and promises made about the treatment of personal data in the target’s published privacy policy. 18 For example, the FTC has made clear that it views the failure to comply with published privacy policies as a violation of Section 5 of the FTC Act. 19 In the European Union (EU), it is noticed the inclusion of the EC’s standard contractual clauses on M&A to avoid potential Data Protection Authorities filings. 20

Therefore, in US law, most of the focus is on the target’s and purchaser’s privacy policies and promises. But in the EU, the focus in review of post-acquisition practices is on the purposes for which the data was initially collected. The use of the data by the purchaser must be in a manner consistent with the specified purposes for which it was obtained by the target in the first place. 21 Apart from the regulatory compliance issues, the costs of integrating databases may be substantial and create transaction risk. Consequently, if the companies involved in the operation don't have an existing data portability infrastructure, it is fundamental to create a data protection “heat map” to identify areas of highest compliance risk on data portability for the target. 22 In that sense, it is important that a transfer or disclosure of personal data may occur in connection with an M&A transaction, including before consummation of the transaction, being advisable for the seller to enter into a data portability agreement with the purchaser concerning such obligations.

(ii) Signing

If after the due diligence phase the parties reach an agreement for the transaction, they will sign a contract, which can be either a share purchase agreement, an asset purchase agreement, or a combination of both. In case specific infringements were spotted during the due diligence process, the buyer will have to consider whether it expects the seller to remedy such breaches pre-closing, or to bear fines or damages related to them. If an identifiable risk, such as lack of

19 Id.
20 Id.
21 Id.
22 Hogan Lovells, supra note 5, at 4.
data processing agreements, is spotted during the due diligence phase, a price correction or a specific indemnity could be a solution.23

Due diligence of a potential target is necessary to ensure compliance at a target level, being fundamental to have strong and well negotiated confidentiality agreements and non-disclosure agreements.24 If personal data is shared outside of the EU under a non-disclosure agreement, compliance with an adequate level of protection, standard model clauses, and data portability will need to be assessed.25 Consequently, a previous data portability infrastructure between the parties involved in the operation would alleviate the need for interoperability standards agreements during this phase, reducing the risks of data transfer, avoiding data protection issues and complying with international data protection laws, which would facilitate cross-border data transfer as it would be easier to be internationally compliant if a stricter legislation is followed.

(iii) Between Signing and Closing

Integration between signing and closing may require the transfer of personal data between seller and buyer prior to the closing. But the scope of information at this moment can be sanctioned under gun jumping. For integration projects involving large amounts of data, buyer and seller may consider creating a governance framework to ensure that data protection concerns are reflected during each stage of the process. Under the principle of accountability, the seller must be able to register that data protection principles were conscientiously applied throughout the process, and what safeguards have been implemented to ensure that the whole process is reversible if the closing does not occur, which can be set through a data portability infrastructure that allows the vice-versa free flow of data transfer.26

During the period between signing and closing, antitrust authorities may request additional information.27 If the parties’ businesses involve the collection and aggregation of significant

---

25 Id.
26 Hogan Lovells, supra note 5, at 8.
27 Inge Graef et. al., supra note 17, at 1390 (exemplifying that the EC, in its Facebook/WhatsApp merger decision made clear that it had not found any evidence suggesting that data portability issues would constitute a significant barrier to consumers’ switching in the case of consumer communications apps. “Even though the [EC] did not consider restrictions on data portability to constitute barriers to switching in the specific circumstances of the case, the fact that these issues were investigated under merger review illustrates the potential of competition law to address data portability.”). See also Daniel Ilan et. al., supra note 18 (explaining that in the US, “Although at the
amounts of customer data, it is important to analyze whether the combination of those data sets creates a competitively significant barrier to entry that could harm competition. Parties in transactions involving a combination of large sets of user data should be prepared to address potential arguments that the deal will foreclose or undermine smaller competitors. A data portability policy could inform antitrust authorities about efforts made by parties to reduce lock-in effect and switching costs.

(iv) Post-closing

Acquiring data assets through an acquisition does not automatically give a buyer rights to use the data. For example, in the US, regulators have made clear that buyers must continue to honor the privacy commitments made by the seller before closing. In the EU, the post-closing data processing operations are generally part of a broader set of technical and operational services covered by a transitional services agreement. After closing, the parties to the transaction will generally have to continue migration and integration efforts, a process that can last up to two years. As part of transaction integration, parties will need to assess how data protection policies and practices of the acquirer and the target can be aligned, integrating the acquired businesses into the buyer’s data protection governance arrangements.

Under US law, a decisive factor in analyzing the legality of a transfer of personal data will be the promises contained in the target’s published privacy policy. In the EU, a transfer of...
personal data at closing as part of an M&A transaction requires showing that at least one of the grounds for transfer is found. Additional steps may have to be taken in the case of transfers of data outside the European Economic Area (EEA). EU law imposes stringent regulatory constraints on the transfer of personal data outside the EEA to a country that is not deemed to have an adequate level of data protection, which includes the US, unless the transfer is to a company having self-certified under the EU-US Privacy Shield. Therefore, a data portability policy should also be developed after post-closing, since it would benefit users of M&A companies who would like to migrate their data and reduce problems in international trade, as the transfer of international data could face restrictions under data protection regulations, such as the GDPR, which requires an adequate level of data protection from countries outside the EU.

3. Conclusion

Considering the efficiencies of a previous data portability policy and infrastructure between the companies entering into an M&A process, prior to signing, a purchaser’s due diligence will involve a risk analysis of transfer and disclosure of data related to the M&A transaction. The seller should consider entering into a data portability agreement with the purchaser with respect to such obligations, defining and categorizing the types of data related to the operation identifying which data should be considered portable before the M&A transaction, as well as running a comparative test confronting the M&A’s portability risks in light of data protection compliance. On signing, the parties should perform a deep examination of the data portability infrastructure between the companies to reduce the risks of data transfer and comply with international data protection laws. Between signing and closing, a thorough data portability report, which can be made under a data protection impact assessment, and a risk assessment related to data transfer should be made to inform antitrust authorities about efforts made by parties to reduce any lock-in effect and switching costs. After the transaction closes, it is

34 See Franz Urlesberger, Does the Right to Privacy Play any Role in Merger Control Proceedings?, Schonherr Blog (2018), https://www.schoenherr.eu/publications/publication-detail/does-the-right-to-privacy-play-any-role-in-merger-control-proceedings/ (showing that “[a]nother recent example of data protection rules coming into play within the competitive assessment came to light during the EC’s assessment of an envisaged joint venture between Sanofi and Google. The joint venture was meant to offer services for the management and treatment of diabetes, including data collection, processing, and analysis. In its competitive analysis, the EC addressed concerns voiced over the ability of the parties to lock-in patients by limiting or preventing the portability of their data towards alternative services. The [EC] dismissed these claims by inter alia pointing to the GDPR, which will provide the users with the right to request portability of their personal data... In light of this, the EC considered the power of locking-in patients to the services of the joint venture to be unlikely in the foreseeable future.”).

35 Daniel Ilan et. al., supra note 18.
important to develop and implement tools for customers and employees to download their data to have data mobility compliant with the most rigorous data protection frameworks across the globe.