

**DIRECTORATE FOR FINANCIAL AND ENTERPRISE AFFAIRS  
COMPETITION COMMITTEE**

**Data Portability, Interoperability and Competition – Note by Israel**

9 June 2021

This document reproduces a written contribution from Israel submitted for Item 1 of the 135<sup>th</sup> OECD Competition Committee meeting on 9-11 June 2021.

More documents related to this discussion can be found at  
<https://www.oecd.org/daf/competition/data-portability-interoperability-and-competition.htm>

Please contact Mr Antonio Capobianco if you have questions about this document.  
[Email: Antonio.CAPOBIANCO@oecd.org]

**JT03476957**

## Israel

In view of the hearing to be conducted this coming June, on the issues of Data Portability, interoperability and competition, attached hereby, is a Policy Paper, published in January 2021 by a Joint Team of the Israel Privacy Protection Authority, the Israel Competition Authority (also, the "ICA"), and the Consumer Protection & Fair Trading Authority (the "Policy Paper", and the "Joint Team", respectively).

The Policy Paper was translated from Hebrew to English, in light of the OECD hearing<sup>1</sup>.

The Policy Paper is one of the first fruits of the Joint Team, established in September 2019 for the purpose of addressing issues arising out of the challenges of the digital economy. The right to data portability is at the core of the issues that are common to the areas of operation of the three Authorities, since it relates to the personal information and privacy field, but has a significant impact on the areas of competition and consumer protection as well.

In the Policy Paper, the Joint Team recommends the adoption of the general right to personal data portability in Israeli law, and specifies the main considerations to take into account regarding such right.

The right to data portability provides consumers autonomy and control over their personal information and restores some balance to the dynamic between consumers and providers of digital services. In addition, the right to data portability is expected to increase competition and the range of options for consumers in digital markets. Data portability makes it easier for consumers to switch between providers, and for new providers to offer tailored products or services based on prior information. Several markets in the digital economy are characterized by a high degree of concentration, and data portability is likely to limit switching barriers in these markets, and thus help to increase competition. These and other benefits of the right to data portability are of greatest significance in view of the growing relevance of the data resource in digital markets.

The general right to data portability has been recognized by various legal systems worldwide, including the European Union in the framework of the GDPR rules, California, Brazil and others. *Inter alia* in view of the accumulated international experience of data portability, as well as academic literature review on the issue and the expected benefits to the Israeli consumer, the Joint Team recommended the adoption of this general right by the Israeli legal system, *inter alia* according to the following principles:

- The right will apply only to personal and digital information, which will be sent to the user in a secure manner;
- The right will be granted at no additional cost to the consumer;
- Information will be transferred to users in a digital, commonly used and machine-readable format, so that it can be used for other purposes;
- The right will apply to certain entities that meet a minimal threshold which will be defined, among other things, according to the scope of their activity and number of customers.

---

<sup>1</sup> The attached, is an unofficial, non-binding translation.

The Joint Team also recommended that, in the case of sectors where data plays a significant role, additional specific regulation should be defined to promote assimilation and implementation of the right.

This Policy Paper was published, for public comments. The Joint Team received commentaries from agents from the academy, private and public sector, and it is currently acting to advance regulation on data portability in the Israeli Law.

## *The Right to Data Portability*

### A Joint Paper

#### 1. Preamble

1. The digital age has, inter alia, given rise to the collection and use of ever-increasing quantities of consumer data, in a way that might substantially alter economic and social conduct all around the world. Data has never been so prevalent; for instance, the volume of data that is produced around the world is expected to increase by a factor of more than 5, between 2018 and 2025.<sup>1</sup> A large variety of bodies rely on the consumer data that is collected in various consumer activities – including browsing the internet, using digital applications and the internet of things (IoT). In this context, the use of consumer data has given rise, and will continue to give rise, to the development of a wide range of products, services and innovative business models, the majority of which are at no (financial) cost to consumers.

2. Alongside the advantages to consumers, the use of consumer data brings with it significant challenges including, inter alia, concerns that arise with respect to protection of privacy and use of the consumer’s personal data in a manner that does not benefit the user, and that might harm the advancement of competition in the various markets. Accordingly, a number of countries have recently legislated or are considering legislating new consumer data rights which are designed, inter alia, to protect privacy and to improve the control that consumers have over their data.<sup>2</sup>

3. As the European Data Protection Supervisor noted in 2014, privacy protection laws, competition laws and consumer protection laws share common goals and interests – including the advancement of growth, innovation and the welfare of individual consumers. Therefore, a closer discourse between the regulators could assist in the enforcement of rules regarding competition and consumer protection in the world of the digital economy, and could also encourage markets to develop services for the improvement of privacy.<sup>3</sup> Similarly, in a 2020 OECD document on the issue, it was stated that in order to promote better results for consumers on markets that contain consumer data, it is necessary to strive for collaboration between the governmental institutions that are responsible for these three areas of the law.<sup>4</sup>

4. In light of the above, and taking into account the fact that certain questions regarding the digital economy are, to a considerable extent, to be found in the intersection of these three sets of laws, in recent years, joint teams have been set up in various countries

---

<sup>1</sup> European Commission (COM/2020/66), *A European Strategy for Data 2* (2020) (hereinafter: **A European Strategy for Data**).

<sup>2</sup> OECD (DAF/COMP(2020)1), *Consumer Data Rights and Competition - Background Note 5* (2020) (hereinafter: **OECD, Data Rights**).

<sup>3</sup> European Data Protection Supervisor, *Privacy and Competitiveness in the Age of Big Data: The Interplay between Data Protection, Competition Law and Consumer Protection in the Digital Economy* (2014).

<sup>4</sup> OECD, *Data Rights*, at p. 41.

around the world, in order to deal with them.<sup>5</sup> In fact, in some countries, the same regulatory authority is responsible for more than one area, in a way that enables continuous integration between the fields.<sup>6</sup>

5. Similarly, in Israel too, in 2019, the Competition Authority, the Consumer Protection and Fair Trade Authority and the Privacy Protection Authority (hereinafter jointly: the **Authorities**) set up a joint team to deal with central questions in the field of the digital economy (hereinafter: the **Team**) with the aim of advancing and ensuring the protection of the substantial and related public interests for which the Authorities are responsible.<sup>7</sup> In the background to the establishment of the Team was the understanding that the digital economy gives rise to significant questions relating to issues of consumerism, competition and privacy, inter alia in light of the growth of the internet giants and the increasing power of social networks and various digital platforms. This is particularly clear in the era of big data, where there are economies of scale for entities that hold greater amounts of data about consumption and consumer preferences.

6. In the course of the Team's work, this paper has been formulated, dealing with the right to data portability – a right that enables a private individual to ask to be provided by digital means (and sometimes, for a third party to be provided, directly) with data collected with respect to him by a particular entity, so that additional or repeat use of the data might be able to be made. This right is at the core of the issues that are common to the areas of operation of the three Authorities. As shall be set out in greater detail below, the source of the right to data portability lies in the field of privacy – due to the fact that it relates to personal information – but it has a significant impact on the fields of competition and consumer protection as well.

7. As shall be set out below, this is an issue that is on the agenda of several developed countries, that has been reviewed in the literature and that has been implemented as policy in various places from whose experience we can, to a certain extent, learn.

8. The structure of this document is as follows: Chapter (B) will present the right to data portability and briefly review part of the application of the right in various countries around the world; Chapter (C) will set out the rationales and purposes behind the right in the view of the three relevant areas of the law; Chapter (D) will set out the principal considerations and challenges that need to be taken into account when setting the right, as well as the Team's principal recommendation for each of them with respect to implementation of the right in Israeli law; Chapter (E) will summarize the document and point to possible advancements in this matter.

---

<sup>5</sup> See, for instance: Personal Data Protection Commission in Collaboration with Competition and Consumer Commission of Singapore, *Discussion Paper on Data Portability* (2019) (hereinafter: **Data Portability, Singapore**).

<sup>6</sup> Examples of this are: the Federal Trade Commission (FTC) in the United States of America, the Australian Competition and Consumer Commission in Australia, the Competition and Consumer Authority in Finland and the Competition and Consumer-Commission in Singapore.

<sup>7</sup> For more, see the articles by the Competition Authority and the Privacy Protection Authority on this subject: [https://www.gov.il/he/departments/news/digital\\_economy\\_news](https://www.gov.il/he/departments/news/digital_economy_news); <https://www.gov.il/he/departments/news/press-cooperation>.

## 2. The Right to Data Portability

9. In general, the right to data portability provides consumers with the possibility of obtaining the data collected with respect to them by a particular entity, and to transfer such to another entity, either indirectly or directly.<sup>8</sup> In this way, the consumer can copy and transfer personal data easily from one computing environment to another, to control the data collected with respect to them and to make additional use of it in accordance with their needs.

10. As it is usually defined in laws around the world, the right to data portability states that a person who holds personal data (hereinafter: a **data controller**) about a person (hereinafter: the **data subject**)<sup>9</sup> which is provided to the data controller by the data subject shall transfer the data in a machine-readable format, by digital means, to the data subject (and sometimes directly to a third party acting on his behalf as well) at his request, in a manner that enables reuse or additional use of the data. After receipt of the data, the data subject may make use of the data as he sees fit.

11. During the past decade, a number of private voluntary initiatives have been developed around the world that are designed to encourage data portability, mainly in specific sectors. Examples of this are the US government series of My Data initiatives which were launched in 2020, which enable access to data that is held, inter alia, by government agencies in various fields. Some of these initiatives were even made jointly with private entities, such as the “Green Button” initiative in the field of energy and electricity, and the “Blue Button” initiative in the field of health.<sup>10</sup> In 2011, the Government of Great Britain launched the Midata Initiative – a data portability initiative that was established in collaboration with various industrial entities, mainly in the field of energy, finance and mobile telephones.<sup>11</sup>

12. Later on, in recent years, a general right to data portability has been established in various countries, in the context of which particular entities are required to provide the personal data in their possession to the data subject, at his request. This was done, for instance, as part of the legislative reform that took place with respect to protection of data and privacy in the European Union in 2016, at the center of which was the General Data Protection Regulation (hereinafter: the **GDPR**) which came into force during the course of 2018. Section 20 of the GRPR prescribes a general right to data portability.<sup>12</sup> In the State

---

<sup>8</sup> Jason Furman, et al., *Unlocking digital competition: Report of the digital competition expert panel* 65 (UK government publication, HM Treasury, 2019) (hereinafter: **Furman**).

<sup>9</sup> For the sake of convenience, throughout this document, we shall also use the terms “customer” or “consumer”.

<sup>10</sup> Kristen Honey et al., *My Data: Empowering All Americans with Personal Data Access* (2016) <https://obamawhitehouse.archives.gov/blog/2016/03/15/my-data-empowering-all-americans-personal-data-access>.

<sup>11</sup> Department for Business, Innovation & Skills, *The Midata Vision of Consumer Empowerment* (2011) <https://www.gov.uk/government/news/the-midata-vision-of-consumer-empowerment>.

<sup>12</sup> Section 20 of the GDPR provides, inter alia, as follows: “The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided ...”.

of California, USA, as well, the California Consumer Privacy Act (hereinafter: the **CCPA**) was enacted in 2018, in which the aforesaid right was also set out.<sup>13</sup>

13. Alongside the general right to data portability, a specific right to data portability has been set in some countries, which is applied to specific sectors only, and is mostly applied via a uniform standard. That is in order to enable the faster and more efficient transfer of data between the various entities that operate in the sector. Thus, for instance, in the European Union, as part of the Revised Payment Services Directive (EU) 2015/2366 (hereinafter: the **PSD2**), banks are required to allow third parties access to the payment account data of customers, subject to their consent. Similar arrangements also exist in other fields in the European Union, inter alia in the field of electricity and smart meters.<sup>14</sup> In Australia too, the right to data portability, which is known as the Consumer Data Right (CDR) is not applied to the entire market but rather, only to specific sectors, and in a gradual manner. The right has initially been applied in the banking sector, with the aim of creating open banking, and it will later also be applied in the field of energy and communications.<sup>15</sup>

14. In Israel, similar processes can be seen to be at their inception in specific sectors. With respect to the financial sector, on June 24, 2020, a Memorandum of the Financial Data Services Provision Bill, 5780-2020 was published (hereinafter: the **Memorandum of the Financial Data Bill**). The proposed arrangement, which is based, to a considerable extent, on PSD2, enables bank customers and credit card companies to share their financial data with third parties. New players, and not necessarily banks, will be able to access the information in the customer's bank account, with his consent, and offer him banking services that are tailored to his needs (at first, the Law will apply to the banking field, with the option of expanding it to the entire financial sector to be examined later on). It has also been prescribed that the secured technological mechanism for transferring the data of service providers that have different sources of data is to be uniform, and is to be based on the European working framework. The proposed arrangement prescribes provisions that relate, inter alia, to preservation of the privacy of customers and to the securing of their financial data. In addition, as was set out in the Explanatory Notes to the Memorandum, "the access to the financial data of a customer that is in the possession of financial sources of information is expected to remove switching barriers between various financial service providers and to encourage competition, both on the demand side and on the supply side".<sup>16</sup>

---

<sup>13</sup> Section 1798.100(d) of the CCPA provides, inter alia, as follows: "A business that receives a verifiable consumer request from a consumer to access personal information shall promptly take steps to disclose and deliver, free of charge to the consumer, the personal information required by this section. The information may be delivered by mail or electronically, and if provided electronically, the information shall be in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit this information to another entity without hindrance ...". Note that a general right to data portability also exists, inter alia, in Brazil – section 18 of the General Data Protection Law (hereinafter: the **GDPL**); Thailand – sections 24 and 31 of the Personal Data Protection Act; and the Philippines – section 18 of the Data Privacy Act. Furthermore, various countries including Singapore and India are in the process of legislating such a right. The OECD recently noted that work is currently taking place on a project that is designed to examine the implications and influences of the right to data portability in a manner which will certainly help to deepen the discourse on this issue. See: OECD, Data Rights, at p. 6.

<sup>14</sup> See, in this context: Directive 2019/944; Commission Regulation (EU) 2017/1485; Commission Regulation (EU) 2015/703.

<sup>15</sup> The right to data portability in Australia – the Consumer Data Right (CDR) – is anchored in the legislative amendments that were made to the Competition and Consumer Act and the Privacy Act.

<sup>16</sup> The Memorandum of the Financial Data Bill, at p. 6.

15. In the field of energy, on July 2, 2020, the Electricity Authority published a hearing on the question of the principles for the management of data in the electricity industry in which it clarified, inter alia, that the purpose of the hearing was to ensure the transfer of information between the various players in the economy, in accordance with a consumer request.<sup>17</sup> In this context, the Electricity Authority noted that as a rule, the consumer is the owner of the personal data collected with respect to him, and noted the importance of regulating data management.

16. As shall be set out below, there is naturally no uniformity between the details of the rights prescribed in the various countries, inter alia in terms of the scope of the right prescribed, exceptions to the right and the method of implementation of it. However, it would appear that the rationales and the purposes on which they are based are identical, and accord with the general vision that is behind the establishment of the Team.

### 3. The Rationales behind the Right to Data Portability

17. The OECD describes four main goals that form the basis for the right to data portability, which are based, inter alia, on the various initiatives that have, to date, been implemented around the world, including the examples above.<sup>18</sup> These goals each, in their own way, clearly connect to the central purposes that each of the Authorities also advance.

#### 3.1. "Self-determination" of Personal Data

18. The right to data portability enables private individuals to exercise their own control of their personal data. Data portability is intended, first and foremost, to provide individuals with greater autonomy and control over their own data and what is done with the data collected about them; and as a result of that, to also assist in balancing the power relationship between consumers and the providers of digital services.<sup>19</sup> This purpose accords with the purposes of privacy protection laws and consumer protection laws which are designed, inter alia, to empower data subjects and to provide them with the possibility of managing what is done with their personal data.

19. In general, the basic presumption of consumer legislation is that the contractual relationship between the consumer and the business takes place in an arena that is fundamentally unbalanced. The business is an informed commercial entity in an advantageous position whilst the household consumer is a single individual who is inferior in terms of information and who does not usually enjoy any real bargaining power against the business. The purpose of consumer protection laws is to enable consumers to make informed decisions and to ensure that they have the power to choose on the basis of full information, without pressure from businesses. The ability of a consumer to move easily between one business and another strengthens and increases the consumer free and

---

<sup>17</sup> The Electricity Authority, Hearing – Principles for Electricity Data Management (July 2, 2020).

<sup>18</sup> OECD, *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies* (2019), and the references mentioned therein (hereinafter: **Enhancing Access to and Sharing of Data**).

<sup>19</sup> It would appear that with respect to data and privacy on the internet, consumers were indeed interested in greater control. A comprehensive study on this topic, which contained a number of extensive surveys, confirms these claims. For instance, the researchers discovered that in many cases, consumers are not even aware of the fact that they are sharing data when using digital measures. See: Jay P. Kesan et al., *A Comprehensive Empirical Study of Data Privacy, Trust, and Consumer Autonomy*, 91 IND. L. J. 267, 294(2016) (hereinafter: **Kesan et al.**).



informed choice to remain in a transaction, or to depart from it. Apart from that, strengthening a consumer's rights in the personal data that is collected with respect to him might help him reduce the information discrepancies between him and the business, and may also enable him to benefit from the data.

20. In addition, a fundamental principle in privacy protection law is the granting to the data subject of a right of access to personal data collected about him and held by another entity. In Israel, this right is recognized as the "right of access",<sup>20</sup> which enables an individual to access the data kept about him on a database.

21. However, the significant increase in the quantities of data that a data subject provides, or that are generated with respect to him as part of the consumer's use of online services makes it hard to extract personal data from the various types of data that are kept by service providers and database owners. The abundance of digital information gives rise to a difficulty in enabling the data subject to access the data efficiently in a manner that might be useful and meaningful for him. The right to data portability is designed to ensure that the rights to privacy of the data subject are not divested of content in the invasive digital environment, and it constitutes a response to the developments that have taken place in the digital economy – and in particular, the increase that has arisen in the collection and use of data. The right to data portability therefore expands the right that currently exists in Israeli law and is more suited to the current digital era.

22. That means that the right to data portability supplements the right to receive access to data by granting the data subject the right to request transfer of the data to him or to a third party, in such a way as to enable the making of additional uses of the data, at the wish and request of the data subject.

### 3.2. Increasing Competition and the Variety of Options for Consumers

23. Fast and efficient data portability is expected to increase the level of competition and the field of opportunities available to consumers in digital markets. In general, quite a few markets in the digital economy are characterized by high levels of centralization. Despite some early forecasts predicting that the internet would create competitive markets – or even perfect competition<sup>21</sup> – in fact, in many cases companies in certain digital markets have managed to attain significant market power and to preserve it over time.<sup>22</sup> Significant

---

<sup>20</sup> See section 13 of the Protection of Privacy Law, 5741-1981, which deals with the right of access of data. In addition, see Directive No. 7112/1 of the Registrar of Databases regarding application of the provisions of the Privacy Protection Law to the right of access of sound and video recordings, and other digital data: [https://www.gov.il/BlobFolder/policy/right\\_of\\_access/he/video.pdf](https://www.gov.il/BlobFolder/policy/right_of_access/he/video.pdf); and Directive No. 2/2012 of the Registrar of Databases.

<sup>21</sup> See, for instance: Erik Brynjolfsson & Michael D. Smith, *Frictionless Commerce? A Comparison of Internet and Conventional Retailers*, 46 MGMT. SCI. 563, 563 (2000), where the authors believe that: "The conventional wisdom regarding Internet competition... is that the unique characteristics of the Internet will bring about a nearly perfect market"; Jeffrey R. Brown & Austen Goolsbee, *Does the Internet Make Markets More Competitive? Evidence from the Life Insurance Industry*, 110 J. POL. ECON. 481, 482 (2002), where the authors believe that: "The traditional economic view suggests that . . . the Internet should reduce search costs for consumers and thereby reduce prices and make markets more competitive".

<sup>22</sup> Among the conclusions that arise in a study dealing with privacy on the internet is that one of the reasons why there is a difference between what consumers would like with respect to privacy on the internet and the way in which they in fact behave is that there are no significant alternatives and the market has no incentive to provide any. Therefore, the authors' recommendation to regulatory

innovative digital industries such as search engines, social networks, network operating systems, electronic trade and shared transportation are generally considered to be fairly centralized industries that are controlled by a small number of companies.<sup>23</sup> There are a number of characteristics of digital markets that might help in the development of a centralized market, including, inter alia, the “network effect”, economies of scale, and economies of scope.<sup>24</sup> In this regard, fast and efficient data portability might somewhat reduce the concerns that arise due to these characteristics, and might, in various ways, increase the competition between the providers of digital goods and services, and the field of opportunities available to consumers in the relevant markets.

24. Firstly, data portability might significantly reduce the switching barriers in various digital markets. As can be seen from the economic literature, where there are high switching costs in a market, the level of competition is lower and companies in the market are able to set a high price level.<sup>25</sup> Incumbent companies have no incentive to reduce prices even where there is an expectation of the entry of new players onto the market, due to the knowledge that their chances of losing customers is small, due to the switching barriers that the consumers face.<sup>26</sup>

25. Personal data might be a significant switching barrier in data-driven markets since consumers will be concerned that switching to a new supplier might cause a loss of the historical data that has been accumulated, such as photographs, search history, the tracking history of certain activities, applications, etc.<sup>27</sup> In this context, data portability is expected to increase competition and to provide an advantage to small or new players joining in, by reducing switching costs. In addition, it will empower the consumer, who will no longer find himself “locked in” to a particular company.<sup>28</sup> Thus, if a particular customer is not satisfied with the level of price, service or quality that the company with which he contracted is providing him, data portability will enable him to switch to a competing company more easily.

---

entities is to create a way of involving consumers in decisions relating to their data. See: Kesan et al., at p. 352.

<sup>23</sup> Furman, at pp. 24-31.

<sup>24</sup> For more, see: Furman 32-37 and the citations therein.

<sup>25</sup> The term “switching costs” is a generic name for any kind of cost that is forced upon a consumer if he wishes to replace a particular supplier to which he is connected in order to obtain a particular product or service. These costs can be financial, but can also be measured in terms that are not material (for instance, costs for learning, time, effort, concern of loss of data, etc.). They might cause the consumer to be concerned about harm to his lifestyle and therefore, the existence of them harms the chance that the consumer might switch suppliers. Therefore, a switching cost limits the consumer’s ability to choose and might constitute a competitive barrier. For more on this see: Thomas A. Burnham et al., *Consumer Switching Costs: A Typology, Antecedents, and Consequences*, 31 J. ACAD. OF MKTG. SCI. 109 (2003);

<sup>26</sup> Paul D. Klemperer, *Price wars caused by switching costs*, 53(3) REV. OF ECO. STUD. 405 (1989).

<sup>27</sup> See, for instance, the Decision of the Bundeskartellamt which was handed down in 2019 in the case of Facebook, in which it was held, in paragraph 469, that in the relevant market, the lack of data portability constitutes a switching barrier for consumers: Bundeskartellamt (Feb. 6, 2019), B6-22/16, (hereinafter: **Bundeskartellamt (Feb. 6, 2019)**). Note that an appeal is pending against this Decision.

<sup>28</sup> Michael Wohlfarth, *Data Portability on the Internet*, 61(5) BUS. & INFO. SYS. ENG’G 551 (2019); Data Portability, Singapore, at p. 12.

26. Secondly, data portability might help in lowering the entry barriers of potential players and in expanding small players in a particular market. That is particularly the case where personal data is a significant resource and new players have difficulty obtaining it. In a data-driven market, small companies mostly have a smaller database than larger companies. Therefore, the collection, analysis and processing of large quantities of consumer data can provide companies operating in digital markets with a competitive advantage, in a manner that makes it hard for new players to penetrate the market.<sup>29</sup> The option of data portability might, therefore, facilitate the entry of potential players and the expansion of existing small companies.<sup>30</sup>

27. Competition authorities around the world have also found that a lack of data portability can raise entry barriers into a number of digital markets; inter alia, the Bundeskartellamt, in the Decision in the Facebook Case,<sup>31</sup> and the Australian Competition and Consumer Commission (ACCC) in the Inquiry that it issued regarding digital platforms.<sup>32</sup> The ACCC also emphasizes, inter alia, the importance of consumer data in improving the services offered and in attracting new consumers (the “feedback loop”).<sup>33</sup>

28. Thirdly, the greater the awareness of consumers as to the importance of the data being held by these companies with respect to them, the more the asymmetry between suppliers of goods and services and their customers will reduce. A higher level of transparency could help customers compare and choose the products that they are interested in. The lack of control and lack of access of consumers to the data held by various corporations and companies with respect to their consumption patterns and preferences increases the information gaps between the private consumer and the business.

---

<sup>29</sup> Katharine Kemp, *Concealed Data Practices and Competition Law: Why Privacy Matters*, UNSW Law Research Paper No. 53-19 (2019).

<sup>30</sup> From a similar point of view, data portability enables new players to offer potential advertisers more targeted advertising, in such a way as to increase competition with existing companies in the market. But for this data, some businesses might not have economic feasibility due to limited forecast revenues. In fact, the revenues that come from targeted advertising are sometimes the principal source of revenue for many digital companies (which often offer their services at no cost to consumers), and this might be more profitable for them than traditional payment mechanisms. For more, see: Moritz Böhmecke-Schwafert & Crispin Niebel, *The General Data Protection’s (GDPR) Impact On Data-Driven Business Models: The Case of the Right to Data Portability and Facebook*, 2 ITU J. (2018).

<sup>31</sup> Bundeskartellamt (Feb. 6, 2019), paragraph 482, where it was held as follows: “The high competitive relevance of the data base to a supplier of social networks will, however, create an additional barrier to market entry ...”.

<sup>32</sup> ACCC, *Digital Platforms Inquiry: Final Report* (2019), where it was noted, on page 11, as follows: “The breadth and depth of user data collected by the incumbent digital platforms provides them with a strong competitive advantage, creating barriers to rivals entering and expanding in relevant markets, and allowing the incumbent digital platforms to expand into adjacent markets ...”.

<sup>33</sup> In this context, see also: Giuseppe Colangelo & Mariateresa Maggolino, *Data Accumulation and the Privacy-Antitrust Interface: Insights from the Facebook Case for the EU and the U.S.*, Stanford Law School and the University of Vienna School of Law TTLF Working Paper (2018): “the collection and aggregation of data, including personal data, by dominant firms entrenches their dominant positions ... the more data a firm gathers and analyzes, the better its products, the more users it attracts, the more data it collects and processes, and so on”.

### 3.3. Encouragement of Data-Driven Innovation and Product Development

29. Data portability might encourage data-driven innovation and the development of new products, accordingly. Data is an essential resource for development of the economy and constitutes a basis for many products and services.<sup>34</sup> Apart from that, the personal data of consumers and knowledge of their preferences enable the tailoring of products and services to their needs. Therefore, in addition to the promotion of competition in the markets to which the consumer's data itself relates, data portability might also encourage innovation as a result of the collection of newer and more varied data by companies. With larger quantities of data, companies in data-driven markets can improve their products or penetrate new markets. And all of that in a way that will benefit the end consumer and contribute to his welfare.

### 3.4. Facilitation of Data Flow and Sharing

30. The right to data portability might constitute a significant step for the promotion of the freer flow and sharing of data. The possibility of data portability might increase the trust of users and, as a result, might increase their willingness to provide additional data to the service providers with whom they contract. Implementation of the right might also assist in overcoming existing barriers to the sharing of personal data because individuals will have better control of their data and will be able to make more efficient decisions as to how and to whom to provide it.

31. In this context, it should be noted that the level of consumer privacy might improve as a result of the right to data portability. If the adoption of the right enables a relatively easier switch to other companies, consumers will be able to leave platforms that do not respect user privacy and switch to platforms that provide greater privacy. In this way, the right to portability might, therefore, encourage new and existing players to improve the way in which they protect personal data and the privacy of their users. Thus, it will also be possible to increase the standards of service in the field of privacy protection. Furthermore, the right to portability might prevent data loss in the event that a service provider is expected to cease operations. The data subject can ask to transfer the data to a new supplier without losing the data gathered with respect to him.

32. As was noted at length above, data becomes an essential resource in many markets and in particular, in digital markets. A significant and effective sharing of data, and the turning of data into a tool that is not concentrated in the hands of only a few, will contribute to the advancement of the market and an improvement in the services that are offered on it.

33. It is clear that in light of the importance of the purposes that have been set out for dealing with some of the challenges posed by the digital economy, which, as a rule, overlap the purposes of the Authorities; and given the adoption of this policy in various places around the world, the Team believes that **there is room to prescribe a right to data portability in Israeli law**. Alongside that, this is not the end of the discussion, but rather, merely the start, since there are substantial challenges and considerations which must be met with respect to designing the way in which this right will be adopted. And all of this so as to ensure maximum efficiency in the implementation of it.

---

<sup>34</sup> For more on the importance of the data that is available for the development of the economy, see: A European Strategy for Data, at pp. 2-4.

## 4. Considerations that must be Taken into Account when Formulating a Data Portability Policy

34. Alongside the common rationales that gave rise to the advancement of various data portability initiatives around the world, the way in which the implementation of each of these initiatives was set is different from a variety of aspects. The method of implementation of the right in Israel, and the determination of the characteristics of it, are of very real importance with respect to the changes that it might generate for consumers and the achievement of the purposes on which the legislation of it is based. We shall now review the central and most significant considerations that need to be taken into account when formulating a data portability policy in Israel.

### 4.1. Setting of a General or Sectoral Right to Data Portability

35. In general, it would appear that a general right to data portability and a sectoral right to data portability in fact complement one another. The general right recognizes the fact that the individual has rights in the personal data collected with respect to him by various entities, and gives him control and autonomy over such data.<sup>35</sup> In that way, it forms the basis for a dedicated regulatory provision in the specific sectors that rely on the data in their operations, which will ensure practical and effective application of the right. And all of that in a way that will increase the benefit to the consumer and will contribute to the increase in competition in those areas.

36. An historical examination shows that in certain cases, a right to data portability is first set in specific sectors in which the characteristics of the market led to a significant need to establish it, and sometimes, a general, sweeping, cross-sectoral right was legislated thereafter. Thus, for instance, in the European Union, prior to the enactment of section 20 of the GDPR which anchored the general right to data portability, the legislature adopted a duty of transfer of data between players in specific sectors in which there was usually some kind of market failure (including the fields of communication, transportation and finance).<sup>36</sup> On the other hand, as was set out above, in Australia, for instance, the right to data portability is limited to certain sectors and there is no general right that applies to the entire market.

37. In Israeli law, which does not, at this stage, include a general right to data portability, there are also specific sectors in which a process of determining a right to data portability have started to be advanced, including in the fields of finance and energy (see Chapter B).

38. Naturally, as a rule, the determination of a sectoral right to data portability might be more effective for the market and the consumer, and might serve to increase the purposes of the general right.<sup>37</sup> That is, inter alia, in light of the ability to ascribe importance to the specific characteristics of the market the subject of the regulation, as well as the ability to

---

<sup>35</sup> It is clarified that the reference to the data subject as the owner of the rights in the data is not intended to rule on the question of the party in whom title to the data vests.

<sup>36</sup> A European strategy for data, at p. 4; Paul De Hert at el., *The Right to Data Portability in the GDPR: Towards User-Centric Interoperability of Digital Services*, 34(2) COMPUT. L. & SEC. REV. 193 (2018) (hereinafter: **De Hert at el.**).

<sup>37</sup> Inge Graef at el., *Spill-Overs in Data Governance: The Relationship Between the GDPR's Right to Data Portability and EU Sector-Specific Data Access Regimes*, TILEC Discussion Paper No. DP 2019-005 (2019) (hereinafter: **Graef at el.**).

set uniform rules for the transfer of data, and clearer standards for players in the market (the importance of which we shall discuss below).

39. In fact, section 40 of the GDPR itself calls to encourage the adoption of internal sectoral rules in order to contribute to implementation of the regulation, taking into account the specific characteristics of the various sectors and the specific needs of small and medium sized companies. Furthermore, the European Commission will open Common European Data Spaces in strategic data-driven sectors in which the effective sharing of data will have an impact of development of the sector and the promotion of consumer welfare.<sup>38</sup>

40. However, we cannot ignore the declarative importance that forms the basis for the setting of a general right to data portability or its ability to contribute and assist various consumers in markets in which there is no specific regulation relating to data portability. Indeed, in light of the challenges that have been presented in this paper, it is possible that the direct impact of a general right to data portability and its ability to achieve the principal purposes on which it is based might be limited; however it would appear that it constitutes an initial basis and that a change is necessary with respect to dealing with the challenges that arise from data in the digital era.

41. Therefore, the Team recommends that **the right to data portability be established as a general right in Israel law. At the same time, in sectors in which data portability is of considerable importance, we shall recommend, in addition, the setting of specific regulation**, particularly in sectors in which there is a specific regulator who can move the matter forward and can draft unique rules.

## 4.2. Setting of a Legal Framework for Data Portability

42. In order to adopt the right to data portability in Israel, it is necessary to determine the legal umbrella under which the right will be included.

43. Firstly, the question arises as to whether there will be room to adopt a duty of data portability or whether what should be prescribed is a voluntary initiative. In several places around the world, it is possible to see that the provision of data to the data subject is voluntary or at least, started out that way. We noted above, for instance, the My Data initiative that was launched in the USA in 2010, or the Midata project that was executed in England in 2011.

44. On the one hand, voluntary initiatives place a lesser imposition on the market as a whole; with consumers who consider the right to data portability to be of importance having the possibility of contracting solely with parties that take part in the initiative, and that provide their customers with a data portability option. On the other hand, it is clear that data portability that is based on a merely voluntary basis will have a more restricted impact and efficacy in terms of both consumers and the market.<sup>39</sup> Apart from that, and this is the main point, if, in terms of policy, it is correct to set a right of data portability, and to recognize the rights of the consumer with respect to the personal data collected about him, the legal status of the right must be anchored and the relevant entities must be required to implement it. This will ensure that the individual's right to data portability is not dependent upon the discretion of the data controllers.

---

<sup>38</sup> A European Strategy for Data, at pp. 21-23.

<sup>39</sup>Peter Swire, *The Portability and Other Required Transfers Impact Assessment: Assessing Competition, Privacy, Cybersecurity, and Other Considerations* 116 (2020). Available at SSRN: <https://ssrn.com/abstract=3689171> (hereinafter: **Swire**).

45. In light of the substantial principle of the need to recognize the right of a private individual to his own personal data, and taking into account the increased importance of the issue in the digital era and the expected positive implications of it in the fields of privacy, competition and consumer protection, **the Team is of the opinion that there is room to establish a right of data portability that will be anchored in legislation.**

46. Another issue relates to the need to determine whether the right will be anchored in the framework of one of the three relevant fields of law, or whether an independent law will be enacted that will combine them. For instance, whilst in Australia, the right to data portability is presented as a right that combines competition law with privacy protection law, in places like the European Union, California and Singapore, the source of the right is in privacy protection laws.

47. In this context, the Team is of the opinion that the basis for the right to data portability is first and foremost the considerations and purposes of privacy protection and consumer protection law, and mainly the giving of control to the data subject over the data collected with respect to him, and the recognition of the rights that are afforded to him with respect to such data.<sup>40</sup> Therefore, **we shall recommend anchoring the right in Israel in the Privacy Protection Law or in the Consumer Protection Law.** The Team's tendency at this stage is to anchor the right in privacy protection laws as has been done in most of the countries that have seen fit to adopt the right into their legal system. However, there are also considerations that tilt the balance towards adoption of the right in consumer protection laws and the Team has not yet formulated a final position in this regard.

### 4.3. The Type of Data that is Included in the Right to Data Portability

48. In general, the right to data portability does not apply to all types of data that is held by the data controller. In this context, it is possible to distinguish between types of consumer data by relying on a number of different characteristics – for instance, the nature and content of the data being collected and the level of ability to identify the data subject.<sup>41</sup> Firstly, taking into consideration the fact that the right to data portability is intended, first and foremost, to empower the data subject and to give him control of data collected with respect to him, **it is agreed that this right applies to personal data only**, i.e., data that is related to a single person who can be identified on the basis of such data.<sup>42</sup>

49. Secondly, it is common to divide the types of data into 'input or voluntary data' – data that consumers provide about themselves – such as the filling in of a questionnaire as part of a process of registration on a website or in order to obtain tailored recommendations by a service provider; 'observable data' – for instance, search or viewing history, which is

---

<sup>40</sup> Article 29 Data Protection Working Party, Guidelines on the Right to Data Portability, 16/EN WP 242 rev. 01 (5 April 2017) (hereinafter: **WP29**), at pp. 4-5.

<sup>41</sup> See: OECD, Data Rights, at pp. 7-10.

<sup>42</sup> Section 20 of the – GDPR. For more on the definition of "personal data", see the website of the European Commission: [https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data\\_en](https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en). As shall be discussed below, sometimes personal data will be combined with data about a third party as well, in a manner that might affect the third party's right to privacy. It should also be noted that there might be specific markets in which it is important, mainly for competitive-consumer considerations, alongside the right to data portability, to set a duty of disclosure and transfer of additional data, including aggregative data and unidentifiable data.

automatically collected by the provider;<sup>43</sup> and ‘inferred data’ – combining voluntary data and observable data in order to deduce additional information regarding the consumer, such as areas of interest to the consumer, or family status.<sup>44</sup> Distinguishing between the types of data and defining the types that are subject to the duty of data portability is a central challenge for policy makers and for the entities that operate in the market. For that reason, there is a need to set as clear a rule as possible to enable the division that is necessary in this context.

50. In order to reduce harm to the incentive of innovation and to protect potential proprietary rights of the data controller, the Team is of the opinion that as a rule, **the right to data portability only applies to voluntary data or observable data but not to inferred data.**<sup>45</sup>

51. Furthermore, the challenges that the right is designed to deal with relate to digital markets, and therefore, **the duty of data portability applies to digital data only, and relates to the transfer of such data in a digital format.** Naturally, turning paper documents into digital data involves considerable costs which would be imposed upon the businesses to which the duty will apply, and there is no room to impose a requirement of this kind on private entities.

#### 4.4. The Format in which the Data will be Transferred

52. In order for the right to data portability to in fact reduce barriers faced by customers to switching between various suppliers and to increase competition in the market, the data must be transferred in a format that will enable its reuse. The setting of a format for transferring the data in accordance with these conditions is no trivial task. One of the main barriers to the implementation of data portability and to the effective reuse of data is the lack of common standards for data transfer.<sup>46</sup>

53. The generation of data interoperability (the ability of a system or components to exchange data and make use of the data that is exchanged) between various entities is the key to exploitation of the value of the data and transfer of the data in a format that enables reuse by the transferee. On the other hand, the imposition of significant duties on private entities with respect to the development of particular technology for the purpose of transferring data and ensuring the purposes on which the data portability right is based could impose a heavy onus on such entities, and harm the development of the market.

54. In this context, it was held in European law that the data being transferred must be “in a structured, commonly used and machine-readable format” in such a way as to enable reuse of the data.<sup>47</sup> In addition, Recital 68 of the GDPR clarifies – inter alia – that data

---

<sup>43</sup> It is possible that some observable data might not be provided consciously by the user, particularly if he does not have full comprehension of the Terms of Service, for instance, tracing a user’s location on an application where location is of no relevance to the outcome, or search history.

<sup>44</sup> Furman, at p. 65.

<sup>45</sup> Similarly to the application of the right to data portability in the European Union: WP29, at pp. 8-9; see also: Jan Krämer at el., *Making Data Portability More Effective For the Digital Economy: Economic Implications and Regulatory Challenges* 8 (2020).

<sup>46</sup> See, for instance: *Data Portability*, Singapore, at p. 18; *Enhancing Access to and Sharing of Data*, Chapter 4; European Commission, *Competition Policy in the Digital Era* 81 (2019) (hereinafter: **Competition Policy in the Digital Era**); Furman, at p. 92; De Hert at el., at p. 200.

<sup>47</sup> Section 20 of the GDPR. For more regarding the data transfer format see: WP29. See also, in this context, the UK Information Commissioners’ Office Guide: <https://ico.org.uk/for->



controllers should be encouraged to develop a uniform standard for transfer of data, but that they must not be required to adopt or maintain suitable technological systems.

55. In the law in California as well, the data controllers are required to provide the customer's personal data "in a portable ... and readily useable format that allows the consumer to transmit this information to another entity without hindrance".<sup>48</sup>

56. It is clear, therefore, that there is a significant difficulty in setting common standards that will apply to the entire market in the context of data transfer, and that it must be recognized that standards differ between the various markets and even within the very same market. Although in some cases, the obstacles that are imposed on data interoperability are technical or might be due to a lack of coordination, in other cases, there is a concern that the obstacles might be due to an incentive not to provide data to existing competitors and to prevent the entry of potential players onto the market.<sup>49</sup>

57. Alongside that, in the case of regulation of data transfer that is focused in a specific sector, it is clear that there is a greater feasibility of the setting of appropriate uniform standards for transfer of the data, either by a designated regulator or by the players in the market itself.<sup>50</sup> These kinds of standards do not ensure only an effective transfer of the data, but rather, also regulate the process of verification and transfer of the data, thereby ensuring data security and the protection of privacy.

58. A good example of that is the implementation of PSD2 in the European Union, a directive that is designed to ensure, inter alia, "open banking". In this context, the European Banking Authority (EBA) published a number of guidelines that were designed to clarify the technical standards for implementation of the Directive,<sup>51</sup> and as a result of that, common uniform standards were developed<sup>52</sup> for Application Programming Interfaces (API).<sup>53</sup> Another example from the private sector is a joint project between Google, Microsoft, Apple, Facebook and Twitter which is known as the Data Transfer Project – which was designed to develop an open source platform for the portability of data between companies.<sup>54</sup>

---

[organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-data-portability/](https://www.fico.org/organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-data-portability/).

<sup>48</sup> CCPA, 1798.100.(d)

<sup>49</sup> Stigler Center, Stigler Committee on Digital Platforms 18 (2019) (hereinafter: **Stigler**), which notes that as a rule, in order to preserve or improve a competitive advantage, businesses have significant incentives to limit openness or interoperability and to object to a data portability policy. See also Furman, at pp. 5-6.

<sup>50</sup> Graef et al., at pp. 18-20; Competition Policy in the Digital Era, at pp. 82-85.

<sup>51</sup> Graef et al., at p. 20.

<sup>52</sup> See: The Berlin Group – A European Standard Initiative, Joint Initiative on a PSD2 Compliant XS2A Interface – NextGenPSD2 XS2A Framework Implementation Guidelines (2018).

<sup>53</sup> API means specifications that are used by software and operating systems and that enable communications between software programs or between software and an operating system. The data is mostly shared between the platforms using API interfaces. For more on the use of APIs as a tool for implementation of the sharing of data in various industries see: Oscar Borgogno & Giuseppe Colangelo, *Data sharing and interoperability: Fostering innovation and competition through APIs*, 35 Comp. L. & Sec. Rev. 1 (2019).

<sup>54</sup> For more see the project website: <https://datatransferproject.dev>.

59. There are also entities including the Internet Engineering Task Force (IETF), the World Wide Web Consortium (W3C) and the Internet Society which are acting to define joint open source standards in digital fields.<sup>55</sup> Note that these organizations depend on the voluntary cooperation of the private companies. However, these kinds of initiatives not only encourage interoperability but might also constitute a basis for future regulation in terms of the setting of standards.

60. In any event, it is clear that the specific sectors in which uniform standards are set for the transfer of data are usually strategic sectors that are based on data for their operation. Therefore, the setting of a uniform format for the transfer of data in these cases and requiring the players in the market to act in accordance with them might impose an onus on such players but, on the other hand, would appear to also provide them with significant business opportunities.

61. In light of the above, the Team is of the opinion that in the context of the right to data portability, **principles that are as clear as possible must be set in light of which transfer of the data will be possible, with the aim of achieving a high level of interoperability. And all of that without requiring the general implementation of suitable technologies.** Alongside that, it is necessary to encourage standard and common formats and protocols for the collection and processing of data from various sources.<sup>56</sup> Furthermore, **in strategic sectors that are based on data for their operation, there is room to consider prescribing specific regulation and developing uniform standards for the method of transfer of data in such market.** The setting of a sectoral policy as aforesaid shall take into account the timing and digital maturity of the entities in the specific market, as well as the existing international standards in the field, in such a way as to enable a cross-border interface.

#### 4.5. Transfer of Data from the Data Controller Directly to a Third Party

62. The possibility of data portability enables the data subject to himself transfer the data received from the data controller to a third party, at his election. Alongside that, there are substantial considerations that support providing the data subject with the ability to ask that the data controller transfer the personal data collected with respect to him directly to a third party, without requiring his intermediation.

63. Firstly, as noted above, from a competitive-consumer point of view, one of the central purposes of the right to data portability is the reduction of barriers preventing customers from switching between different suppliers. Clearly, simplification of the process of switching between suppliers, including reducing the complexity of the transfer of personal information between a number of entities that is necessary for the purpose of such portability, will in fact facilitate the switch and will encourage the customer to do it in cases that are appropriate for him.

64. Secondly, the data subject is the owner of the rights in the personal data collected with respect to him, and there is no reason to prevent him from deciding to whom it will be transferred if, from the point of view of the data controller, the identity of the party to whom

---

<sup>55</sup> Furman, at p. 73.

<sup>56</sup> For instance, in Europe, they set up a national project the principal aim of which is to implement such standard formats. See: <https://ec.europa.eu/digital-single-market/en/news/rolling-plan-ict-standardisation>.

he is transferring the data is of no importance (presuming that such transfer will take place in any event, as aforesaid).<sup>57</sup>

65. Examples exist of both approaches to the direct transfer of data to third parties. Thus, for instance, section 20(2) of the GDPR provides that the data subject has a right to transfer his own personal data directly from the data controller to another party, where such is technically possible. On the other hand, in California, the CCPA provides that the only person who is entitled to receive the data directly from the data controller and to transfer it to another party is the data subject himself.

66. The Team is of the opinion that in order to ensure effective application of the right to data portability and to achieve the purposes of it, there is no room to add stages to the chain of the data transfer process. Therefore, the Team recommends **adoption of the European Union approach so that the data subject is given the right to request transfer of the personal data that exists with respect to him, directly from one party to another**, naturally without derogating from the option of the data subject to transfer the data between such parties himself.

#### 4.6. Scope of Application of the Right to Data Portability

67. As a rule, the right to data portability might increase competition in various markets, inter alia by reducing entry barriers for new players to whom important data is made available which might assist their activities in the market. Notwithstanding the aforesaid, it is clear that the prescription of particular regulation in general, and with respect to issues of privacy and data security in particular, might increase entry barriers to markets and might increase the compliance costs of the various players. In the case of relatively high costs, whether with respect to the initial investment in implementation of the regulation or with respect to the effectiveness of the regulation, a concern arises of harm to the functioning of small players in the market.

68. On the one hand, various players that make use of the personal data of their customers as part of their business model are expected to also comply with minimum conditions for the assurance of the customer's rights with respect to their personal data. On the other hand, the scope of application of the right to data portability will necessarily affect the development of competition in every market. In this context, a concern arises that the setting of a general right to data portability which will be applied to the market as a whole will give rise to the imposition of high adjustment costs on the various players. The imposition of these costs on small businesses might harm competition and, at the end of the day, might also harm the end consumer.<sup>58</sup>

69. The implementation and maintenance of a data portability mechanism, as well as the initial setting up of such a mechanism, involves time and resources. The extent of the investment depends on a variety of parameters, including the amount of data that is required to be transferred, the format in which it is to be transferred, how the data is managed within

---

<sup>57</sup> All of that subject to the existence of security measures that will ensure the preservation of privacy of the data and receipt of the consent of the data subject to effecting the transfer of the data, as aforesaid, as is set out below. Clearly, the cost of implementation of such measures might be a consideration for finding that there is no room to impose a duty of direct transfer of the data to third parties.

<sup>58</sup> Peter Swire & Yianni Lagos, *Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique*, 72(3) MD. L. REV 335, 352 (2013).

the company, etc.<sup>59</sup> As aforesaid, weight must also be ascribed to the expected implications of such costs on competition. In any event, it would appear that the requirement for data portability might give rise to the imposition of an onus that is too heavy, mainly in particular areas such as start-up companies or small and medium-sized businesses that are just starting out, in particular in comparison with more established companies.

70. The OECD has noted that reforms relating to data protection do indeed provide a higher level of privacy and control of data, but might, on the other hand, also harm competition. Therefore, if regulation regarding privacy achieves its targets but, incidentally, reduces competition, such a policy will not necessarily be defined as an overall success, and care must be taken to ensure whether it is not possible to achieve the same goals in a more balanced manner, which will cause fewer distortions to competition.<sup>60</sup>

71. In the academic literature, a possibility has been proposed of granting exemptions from implementation of the right to small and medium-sized organizations that are characterized by relatively small operations turnovers and market shares.<sup>61</sup> In fact, the CCPA is taking that path, contrary to the GDPR which prescribes a general right to data portability which applies to all of the players in the market. Thus, the right to data portability which is set out in the CCPA applies to for-profit businesses that are in compliance with at least one of the following threshold requirements: (a) gross annual revenues in the sum of at least USD 25 million; (b) purchase, sell, receive or share the personal data of at least 50,000 consumers, households or devices each year for commercial purposes; (c) 50% or more of its annual revenues originate in the sale of the personal data of consumers.

72. In order to ensure the delicate balance that is necessary between giving a consumer control of his personal data and the development of competition in markets, we recommend **the adoption of a minimum threshold for application of the duty of data portability with respect to the application of the right**. That is with the aim of exempting small businesses from the relatively heavy onus that is expected to apply to them, taking into account the competitive aspect of data portability.

#### 4.7. The Cost of Exercise of the Right

73. The cost of compliance with the duty of data portability is expected to be significant for some players in the various markets. As a result of that, the question that arises is whether private companies to which the duty of data portability applies should be allowed to collect a fee in consideration for exercise of the right, if only in the sum of the cost of the requested service. The concern that arises is that the cost involved in compliance with

---

<sup>59</sup> See, in this context, the assessments of the cost of implementation of a data portability policy in the banking industry in Great Britain: Data Sharing and Open Data for banks – A Report for HM Treasury and Cabinet Office (2014) -

[https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/382273/141202\\_API\\_Report\\_FINAL.PDF](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/382273/141202_API_Report_FINAL.PDF); and assessments of the costs of implementation of data portability in the banking and electricity sectors in Australia: The Parliament of the Commonwealth of Australia, Explanatory Memorandum, Treasury Laws Amendment (Consumer Data Right) Bill (2019) [https://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r6281\\_ems\\_58a7c56b-36e3-4388-acf8-58455b983a76/upload\\_pdf/698114.pdf;fileType=application%2Fpdf](https://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r6281_ems_58a7c56b-36e3-4388-acf8-58455b983a76/upload_pdf/698114.pdf;fileType=application%2Fpdf)

<sup>60</sup> OECD, Data Rights, p. 43.

<sup>61</sup> Aysen Diker Vanberg & Mehmet Bilal Ünver, *The right to data portability in the GDPR and EU competition law: odd couple or dynamic duo?*, 8(1) European Journal of Law and Technology (2017).

the law will, in any event, be rolled over onto consumers and will be collected from them in indirect ways. Apart from that, presuming that not all of a company's customers exercise their right to data portability, and notwithstanding that, the total cost of the company's products and services increases for all customers as a result of implementation of the right, a situation will arise in which all customers are, in fact paying for a service that only some of them might use.

74. On the other hand, the fundamental presumption on which the right to data portability is based is that the personal data collected by some entity is data in which the customer has rights. The customer, as owner of the rights in the data, may make use of it as he sees fit, including transferring it to third parties. Prima facie, when an entity makes use of the personal data of a customer in the context of its business model, it is also required to provide such person with his rights to protection of the data at no cost, including his right to portability of the data; that is because it would appear to be illogical that a person should be required to pay for his fundamental rights that are prescribed in the law.

75. Apart from that, giving a commercial entity, with whom a customer contracts, the ability to collect a fee for portability of the personal data of the customer that is in its possession might cause harm to the competition that could develop in the market on the basis of the right to data portability. Whether it is the customer who pays such cost or the transfer, it will constitute a barrier to exercise of the right, particularly if significant sums are collected. If the portability process is simple and free, that will increase the incentive that customers have to exercising it.

76. These would appear to be the reasons that led to the general right to data portability around the world being at no financial cost to the data subject. That was the case, for instance, in the European Union in the GDPR, in California in the CCPA and in Brazil in the LGPD.<sup>62</sup> Alongside that, European and Californian law prescribe that there might be certain cases in which it will be possible to collect payment from a customer, particularly when requests for data portability are exaggerated, repetitive, etc.<sup>63</sup>

77. In light of this, the Team's recommendation is **to allow the Israeli consumer to exercise his right to data portability at no financial cost to him, except in extraordinary cases** (such as repeated requests) which shall be prescribed.

#### 4.8. Third Party Data

78. Sometimes, the personal data of a person might be combined with the personal data of other parties. In such cases, the portability of the data of such person gives rise to a concern of harm to the rights to privacy and data protection of the third party. The most obvious case of this is the field of social media, in which a considerable portion of the data might also include the data of a number of users. The question is relevant to these markets in particular, since the value of the data in those markets is prescribed, to a significant extent, by the interactions between the consumers.<sup>64</sup> Therefore, if the right to data portability includes, in this context, a right to the portability of photographs, posts, messages and responses of a third party, it necessarily involves risks to privacy and to the

---

<sup>62</sup> In various sectoral regulations relating to data portability, there is also a prohibition against collecting payment from customers (except in extraordinary circumstances of a high number of requests), such as in the application of PSD2.

<sup>63</sup> Section 12(5) of the GDPR, CCPA § 1798.145.

<sup>64</sup> Gabriel Nicholas & Michal Weinberg, *Data Portability and Platform Competition: Is User Data Exported from Facebook Actually Useful to Competitors?* 3 (2019).

security of the data of third parties. On the other hand, if the transfer of such data is not allowed, there is considerable doubt as to whether the right to data portability will have any meaning or effect in those markets.

79. In this context, section 20 of the GDPR provides that the right to data portability “shall not adversely affect the rights and freedoms of others”.<sup>65</sup>

80. It should be clarified that these issues are less relevant in markets in which the data relates only to private persons, such as consumer preferences relating to the consumption of music, fitness or the watching of videos, and other habits that do not involve other consumers.<sup>66</sup> In sectoral regulation relating to the right to data portability, in sectors that do not include social networks, the personal data mainly relates to the data subject alone and concerns of breach of the privacy of third parties are expected to be less significant.<sup>67</sup>

81. The Team is of the opinion that the path that should be taken is one that is similar to that of European law, with the aim of preventing harm to the privacy of third parties. Naturally, potential solutions to the difficulty presented can be found, inter alia, by obtaining the consent of the third party to portability of the data in advance or specifically, if that party is also a user of the services of the provider.

#### 4.9. Data Security

82. It might be presumed that the setting of a right to data portability will give rise to the sharing of data between entities, sometimes competing entities, at greater frequencies and to significantly greater extents, particularly in comparison with the current situation. The advantages to consumers as a result of that are many and have been set out above. But such a significant increase in data traffic will be accompanied by considerable challenges as well. One of these is data security risks which might arise due to the portability of data between suppliers, and in particular, the increase of the risk of leakage of data and use of the data against the consumer himself. Particularly in the case of different entities that deal in various scopes of data, each of which have different data security systems and risk management systems.

83. Firstly, it is clear that it is necessary to ensure an appropriate level of security at the time of transfer of the data between the various entities.<sup>68</sup> When the data transfer pipeline is not adequately secured, risks to privacy and data security arise due to data leaks in the transfer process. Secondly, care must be taken to ensure data security when the data is in the possession of the original data controller, and the transferee as well. Consumers and organizations must be aware of the potential risks before transferring data to a new suppliers.

84. The greater the magnitude of the personal data that is held by entities, in terms of quantity, variety and format, the more significant the potential damage that might be caused due to data security faults.

---

<sup>65</sup> GDPR, section 20(4).

<sup>66</sup> With respect to cases of the personal data of a third party that is part of the family unit of the data subject or some other relative, it would appear to be possible to find creative solutions for joint consent. See, for instance, section 35 of the Financial Data Services Memorandum which deals with joint accounts.

<sup>67</sup> Swire, at p. 59.

<sup>68</sup> See, for instance: Data Portability, Singapore, at pp. 19-20, and the references mentioned therein.

85. In an ideal world, users are supposed to be cautious when requesting portability of data to a third party, if the third party does not have adequate data security standards. However, it is not enough to rely on users in order to make an appropriate risk assessment. It is most certainly possible that businesses might respond to the market demand for data security measures for portability and might improve the level of their data security, and that consumers will be able to distinguish between companies with respect to levels of data security as well. However, the risk that will not occur is too great and justifies not relying on market forces only, in this regard.

86. Therefore, we are of the opinion that **a policy for data portability must also address data security, as well as setting a mechanism for responsibility and consumer protections for cases in which a data security incident takes place.**

#### 4.10. Policy Adapted to World-Wide Developments

87. The transfer of data between entities in different countries is a critical topic taking into consideration the characteristics of the digital economy and the world of global trade, and particularly since Israel is an important player in the international technology and data markets on the one hand, but a relatively small player on the other hand.

88. In a world in which the transfer of personal data is a necessary, global activity that crosses borders, it is important that the Israeli law be in maximum accord with the law that is in place around the world in general, and in countries with which Israel has trade relations and other relations, in particular. Apart from that, there is also significant importance to be in accord with standards that are being developed for the transferal of data.

89. A large number of Israeli companies that are based on the use of personal data operate in countries other than in Israel, and a large number of similar foreign companies operate in Israel. If the requirements of Israeli law are common to those that are prevalent in other legal systems around the world – particular with respect to countries with which extensive trade relations exist – that will facilitate the legislative adjustments that are necessary for the various companies, and will reduce the regulatory onus that is imposed upon them. The more similar Israeli law is to the international law, it is clear that international companies will have a greater ability to adjust their conduct to the local law, with minimum effort.

90. Taking this into account, **significant weight ought to be ascribed, in making the decision as to the method of acceptance of the right to portability into Israeli law, including when determining the extent and content thereof, to the aspiration of uniformity, as far as possible, with international law on this issue,** as has been done in this Paper.

## 5. Summary and Recommendations

91. This Paper is an initial document which is designed to recommend the advancement of legislation of the right to data portability in Israeli law and to note the principal considerations that ought to be taken into account in enacting such a right.

92. In recent years, a general right to data portability has been prescribed in various countries. Prominent examples of this are the European Union, in section 20 of the GDPR, which came into force in May 2018, and in the State of California in the USA, in the CCPA which came into force in January 2020.

93. The advantages that are expected to flow to the Israeli consumer and market from adoption of the right to data portability are significant, and include the provision of control and autonomy to private individuals over the personal data collected with respect to them by various entities, due to their being the owner of the rights in the data; provision of the possibility to transfer personal data between suppliers in a manner that is expected to reduce the switching costs in various industries, and to increase the competitive pressure by small or new companies vis-à-vis dominant companies; and empowerment of the private consumer vis-à-vis significant entities as well as improving the service provided to them and improving the user experience.

94. However, in order to ensure that the right is effective and achieves its purposes, it must be designed carefully. In this Document, the Team addressed the main issues that relate to acceptance of the right into Israeli law, and it was recommended, inter alia, that a general right to data portability be adopted into the Israeli legal system, with specific regulation also being prescribed in this context in those sectors in which data portability is of considerable importance. The right that will be adopted will apply to personal and digital data only; the data will be transferred in a secured manner; the data will be transferred in a digital, machine-readable and commonly used format, which will enable additional or repeat use of the data; and the right will be granted at no additional cost to the consumer, whether he chooses to transfer the data directly to another entity or whether he chooses to transfer it into his own possession. Furthermore, the right shall also apply to particular entities that are in compliance with a minimum threshold that will be prescribed, inter alia, in accordance with scope of operations and the number of customers.

95. Later on, the Team shall act to advance regulation of the right in Israeli law, inter alia in reliance on the provisions of this Document, on international experience and on the comments of the public that are received in response to the Document.