The New Restriction: Combining Personal Data under the EU's Digital Markets Act and Turkey's Data Protection Legislation

Authors: Gönenç Gürkaynak, Esq., Ceren Yıldız, Yasemin Doğan and Duhan Kurt, ELIG Gürkaynak Attorneys-at-Law

(i) The DMA: New rules for "digital gatekeepers"

European Union's ("EU") Digital Markets Act ("DMA") entered into force on 1 November 2022. The DMA rules apply to the providers of certain pre-defined core platform services that qualify as "gatekeepers". Most of the provisions will be applicable as of 2 May 2023 when the gatekeeper designation procedure will start. Thereupon, providers designated as gatekeepers will have to notify the European Commission ("EC") within 2 months and to comply with a range of obligations and prohibitions within 6 months of their designation as gatekeepers.[1]

To meet the definition of gatekeeper, a company must offer a "core platform service" (CPS) which is defined as online intermediation services, online search engines, online social network services, video-sharing platform services, number-independent interpersonal communication services, operating systems, cloud computing services, web browsers, virtual assistant or online advertising services. A CPS-providing company might be considered a gatekeeper if it meets certain qualitative and quantitative thresholds.[2]

The DMA envisages the imposition of numerous *ex-ante* obligations on gatekeepers with the two main objectives: **(i)** to ensure that digital markets in which gatekeepers operate remain contestable and **(ii)** to ensure fairness and a level playing field for players in digital markets in the EU.[3]

In this context, Article 5 of the DMA imposes a set of requirements directly applicable[4] to gatekeepers including the obligations related to the "combining end-users' personal data". Accordingly, Article 5(2)-b of the DMA requires gatekeepers to "refrain from combining

---

[1] European Parliament, AT A GLANCE, Digital issues in focus, Accessible at https://www.europarl.europa.eu/RegData/etudes/ATAG/2022/739226/EPRS-AaG-739226-DMA-Application-timeline-FINAL.pdf, January 11, 2023.

[2] A provider of CPS shall be designated as gatekeeper if: **(a)** it has a significant impact on the internal market; **(b)** it provides a CPS that is an important gateway for business users to reach end users; and (c) it enjoys an entrenched and durable position in its operations or it could enjoy such a position in the near future. Along with these, quantitative threshold for a company to fall within the DMA's scope are set at €7.5 billion in annual turnover and €75 billion in market capitalization and to provide a CPS with 45 million monthly end users in the EU in the last year and 10,000 business users per year (and **(c)** these criteria have been met in each of the last three years.) Retrieved from European Parliament, Regulating digital gatekeepers Background on the future digital markets act, Accessible at https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/659397/EPRS_BRI(2020)659397_EN.pdf, January 16, 2023.

[3] European Parliament, BRIEFING EU Legislation in Progress, Digital Markets Act, Accessible at https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/690589/EPRS_BRI(2021)690589_EN.pdf, January 16, 2023.

[4] Ibid.

personal data" obtained by CPS with data obtained by any other 1P or 3P services, absent express user consent. Having said that, in Turkey currently there is no specific rule prohibiting the data combination and therefore general rules stipulated under Turkey's Law No. 6698 on the Protection of Personal Data ("DPL") might be applicable to such data combination activities.

(ii) The Restriction on Combining Personal Data under the DMA

Pursuant to Article 5(2)-b of the DMA "*The gatekeeper shall not do combine personal data from the relevant core platform service with personal data from any further core platform services or from any other services provided by the gatekeeper or with personal data from third-party services unless the end user has been presented with the specific choice and has given consent within the meaning of Article 4, point (11), and Article 7 of Regulation (EU) 2016/679*." Therefore, gatekeepers cannot automatically combine consumer data across its different services into a single profile without the relevant consumer's explicit consent. The combination of personal data might become concrete when the gatekeeper adds personal data from a CPS and another relevant service to a user profile to create new insights on that user for the purpose of better personalization of its services. While such obligation aims to ensure that gatekeepers do not unfairly undermine the contestability of CPS, it was criticized for making gatekeeper services less personalized and integrated as well as stipulating to plague consumers with "cookie-banner" style requests for obtaining consent.[5]

Recital 36 also indicates that this obligation reflects a concern that gatekeepers unfairly undermine the contestability of CPS. Further, it explains that Article 5(2) requires gatekeepers to give end users the choice to freely opt-in to such data processing by providing a less personalized but equivalent alternative, without making the use of the CPS or specific functionalities thereof contingent upon the end user's consent.[6]

Accordingly, it might be understood from the wording of the provision that in order to apply consent obligation within the restriction of data combination, there should be **(i)** the "personal data" of the end-user in the meaning of the EU's General Data Protection Regulation (2016/679, "GDPR") **(ii)** the interaction between two different services (one of the services must be CPS) even if both of the services are controlled by one gatekeeper as a whole and **(iii)** no exceptions set out under Article 5(2). Firstly, DMA refers to the GDPR as for the definition of the personal data (as defined in Article 4, point (1), of GDPR)[7]. Therefore, the data outside the scope of the definition of personal data will not be in the scope of such restriction (e.g. anonymized personal data). Secondly, it might be inferred that as the gatekeeper is restricted to add personal data from a CPS and its other relevant service to a user profile, the relevant restriction adopts the concept of service-specific entities that "own" particular data sets, even if both of the services are controlled by one gatekeeper as a whole.

---

[5] Meyers, Zach. "No Pain, No Gain? The Digital Markets Act." Centre for European Reform. Accessible at https://www.cer.eu/publications/archive/policy-brief/2022/no-pain-no-gain-digital-markets-act, January 16, 2023.

[6] Recital 36, DMA.

[7] According to the GDPR, 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Lastly, as an exception, Article 5(2) enables in-scope data processing without consent if there is a basis for data processing under Article 6(1)(c), (d), or (e) of the GDPR[8].
Article 5(2) of the DMA also refers to the GDPR's standard of consent and specifies the consent to be obtained by the end user in this context. As per Recital 37 of the DMA, ***(i)*** *when requesting consent, the gatekeeper should proactively present a user-friendly solution to the end user to provide, modify or withdraw consent in an explicit, clear and straightforward manner,* ***(ii)*** *consent should be given by a clear affirmative action or statement establishing a freely given, specific, informed and unambiguous indication of agreement by the end user, as defined in GDPR,* ***(iii)*** *only where applicable, the end user should be informed that not giving consent can lead to a less personalized offer, but that CPS will otherwise remain unchanged.*[9]
Thus, the DMA outlined how gatekeepers can meet the consent standard. Article 5(2) of the DMA stipulates that if the end user refuses or withdraws the consent for the purposes of data combination, the gatekeeper cannot repeat its request for consent for the same purpose more than once within a period of one year.

(iii) The Restriction on Combining Personal Data under Turkey's Data Protection Legislation

Currently, when evaluating such restrictions in terms of the DPL including the data controller's obligations related to combining personal data, there is no specific rule which clearly prohibits the combination of personal data. Therefore, general rules regarding the processing of personal data and obtaining explicit consent might be applicable for the activities related to the combination of the personal data.

As per Article 3 of the DPL personal data means "*all the information relating to an identified or identifiable natural person*". Article 3 of DPL also defines data processing as "*collection, recording, storage, retention, alteration, re-organization, disclosure, transferring, taking over, making retrievable, classification or preventing the use thereof, fully or partially through automatic means or provided that the process is a part of any data registry system, through non-automatic means*." Moreover, according to the rationale of Article 3 of DPL, the term "processing" must be defined broadly as all types of transactions that are performed on the data from the moment they are first acquired, thus currently as there is no specific rule on data combination, such operations might be subject to the rules regarding data processing under DPL.

Pursuant to Article 5 of DPL, personal data cannot be processed without the explicit consent of the data subject, unless one of the data processing conditions[10] set out in the same article

[8] According to the relevant provisions of GDPR, processing shall be lawful only if and to the extent that at least one of the following applies: c) processing is necessary for compliance with a legal obligation to which the controller is subject; (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person; (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

[9] As per the relevant provision of the DMA, exceptionally, if consent cannot be given directly to the gatekeeper's core platform service, end users should be able to give consent through each third-party service that makes use of that core platform service, to allow the gatekeeper to process personal data for the purposes of providing online advertising services.

[10] Data processing conditions without consent are as follows: (i) it is explicitly foreseen by laws, (ii) processing is necessary to protect the vital interests or the bodily integrity of the data subject or of another person where the data subject is physically or legally incapable of giving his consent, (iii) processing personal data of the parties of a contract is necessary, on condition that processing is directly related to the execution or performance of such contract, (iv) processing is necessary for compliance with a legal obligation which the data controller is subject to, (v) data has been made public by the data subject, (vi) processing is necessary for the establishment, exercise or defence of a legal claim and (vii) processing is necessary for

applies. However, in practice, explicit consent is considered equivalent to the other processing conditions and if there is another applicable processing condition for the processing activity, taking explicit consent is considered unlawful[11].
DPL defines "explicit consent" as the consent on a specific matter which is based on informing and declared with free will. Although explicit consent is not subjected to any form requirement, similar to GDPR, it has conditions i.e. must be freely given, informed, given for a specific purpose, explicit and given via a positive affirmative action, must use clear and plain language, and be clearly visible. Although DPL does not specifically mention withdrawal of consent, explicit consent is considered a right that is strictly attached to the data subject and thus can be withdrawn. In that sense, the data subject can withdraw their explicit consent at any time, however the withdrawal has forward looking consequences as of the moment the data subject's declaration reaches the data controller.

Comparing the rules on data combination between EU and DPL, firstly, as of today, there is no such data combination restriction under DPL. Therefore, currently, gatekeepers might not be required to obtain the consent of the end user if such data combination can be included within one of the legal grounds and data processing conditions stipulated under the DPL. Moreover, currently under Turkish laws, there are not yet any specific rules directly applicable to gatekeepers or CPS in terms of their data protection obligations. Therefore, general terms defined under the DPL such as data controller, data processor, or data subject might still be applicable to the gatekeepers or other service providers in Turkey. Although the definitions of personal data and explicit consent are more detailed in GDPR in comparison to DPL, such definitions are still parallel with each other. Therefore, if the new amendment were to be introduced regarding the prohibition of the combination of personal data in Turkey, the understanding of "personal data" and "explicit consent" might be similar to the DMA.

(iv) Administrative Sanctions

As per Article 30 and Article 31 of the DMA, in case of a failure to comply with the restriction under DMA, the EC may impose on a gatekeeper fine of up to 10% of its total worldwide annual turnover or 20% in the event of repeated infringements and periodic penalty payments of up to 5% of the company's total worldwide daily turnover. In case of systematic non-compliance, the EC may impose additional remedies which might be structural remedies, such as obliging a gatekeeper to sell a business, or parts of it or banning a gatekeeper from acquiring any company that provides services in the digital sector or services enabling the collection of data affected by the systematic non-compliance.[12]

In case of failure to comply with the obligations related to data security (e.g. providing an appropriate level of security for the purposes of: a) preventing unlawful processing of personal data, b) preventing unlawful access to personal data, and c) ensuring the protection of personal data), the data controller shall be imposed to pay an administrative fine of 89.571,04 TL to 5.971.990 TL.

---

the purposes of the legitimate interests of the data controller, provided that such interests do not violate the fundamental rights and freedoms of the data subject.

[11] This is explicitly indicated multiple times by the DPA including their "Data Protection Law Application Guidelines"

[12] European Commission, Press Corner, Questions and Answers: Digital Markets Act: Ensuring fair and open digital markets, Accessible at https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_2349, January 16, 2023.

(v) Conclusion

Although there is no restriction on combining personal data in Turkey as of today, it might be expected that a new legislative arrangement regarding such restriction to be introduced in the near future in line with the DMA provisions.

Article Contact: Gönenç Gürkaynak, Esq. E-mail: gonenc.gurkaynak@elig.com

(First published by Mondaq on January 26, 2023)