e-commercelaw&policy
the monthly journal for online business

Cross-border transfers and on-soil requirements in Turkey

The Protection of Personal Data Law numbered 6698 ('Law') was enacted in Turkey on 7 April 2016, with detailed provisions relating to the protection of personal data. It defines 'personal data' as 'any type of information that relates to an identified or identifiable natural person.' The main principle is that personal data can only be transferred abroad once the data subject has provided explicit consent. However, there are certain exceptions, such as if the processing is clearly mandated by law. This could be where data processing is directly related to the formation or execution of an agreement of which the data subject is a party, or if processing is mandatory for the establishment, use or protection of a right. Furthermore, on the condition that it does not harm the data subject's fundamental rights and freedoms, the processing is mandatory for the legitimate interests of the data controller.

The Law also separately distinguished a category of 'personal data of a special nature,' subject to more extensive protection. The types of personal data that fall under this category include those related to race, political views, security measures and biometric data. The lawmaker has set as a standard a prohibition on transferring personal data of a special nature, unless the explicit consent of the data subject is present. However, excluding health and sex life data, in the situation where data processing is clearly mandated by law, there is no longer a requirement for explicit consent.

In addition, the transfer of data abroad may only take place if there is no need for a data subject's consent or if a foreign country has sufficient safeguards. If the country does not have adequate safeguards, the data controller in the foreign country must provide the data protection institution with adequate protection in writing and ensure that there are equivalent safeguards and that the approval of the data protection institution is obtained. Countries that have sufficient safeguards will be determined by the data protection institution and a list of these countries will be published.

In general, the transfer of data abroad is not prohibited or restricted but rather is subject to certain requirements to ensure that adequate protection is provided in the country where the processing will take place. Importantly, there are certain sectors where transfer of data abroad is not allowed and there are on the ground requirements for operators active in these sectors.

The transfer of data abroad for payment services

The Law on Payment and Security Settlement Systems, Payment Services and Electronic Money Institutions (the 'Law on Payment Systems') requires system operators, payment and electronic money institutions to keep the information related to the requirements set out in the law in Turkey for a minimum of 10 years, in a safe place, whilst offering access to such information at any time. Furthermore, system operators, payment and electronic money institutions must locate the information systems that are used for conducting the services and backups in Turkey.

The rationale behind these rules for payment systems is to protect the users of these systems and to provide security.

As per the Law on Payment Systems, payment and electronic money institutions must obtain a licence from the Banking Regulation and Supervision Authority to provide services in Turkey. There are also a number of other requirements as to the shareholding structure, capital, scope of activity etc set forth under this law. Operators are required to apply to the Authority for a licence within one year from the enactment of the Law on Payment Systems. PayPal failed to obtain the required licence because it does not locate its information systems in Turkey and thus announced the suspension of its services in Turkey.

Locating information systems in Turkey is a requirement specific to the banking sector. However, despite this, it is not a condition applied to every data controller in every sector, considering the sensitivity of protecting the payment information of consumers, such a requirement can be viewed as proportionate. Nowadays it is argued that localisation rules go against globalisation where global trade has no borders and such rules are deemed a hindrance to the global economy. However, considering countries' security and fraud concerns, to a certain extent localisation remains on the agenda in exceptional cases and sectors.

While it is expected that e-commerce sites, online sellers, start-ups and other third parties that direct their transactions predominantly through PayPal will undergo a period of disruption as they attempt to secure alternative payment systems, it is expected that the relevant stakeholders will recover from this situation. There are already reports that PayPal is considering moving the necessary information systems to Turkey so as to be able to re-apply for a licence. Furthermore, as the transition period and the requirements of the legislation have been publically available for some time, there are many companies providing the same services in compliance with the requirements.

In terms of global players, as the transition period imposed under the relevant law for payment institutions was known well in advance, and as key global and local players have secured licences, we do not expect a widespread exit from the Turkish market or a major amendment to the legislation. In fact, it is expected that PayPal may find a way to comply with the requirements and be active in the Turkish market in the future.

Begüm Yavuzdoğan Okumuş Managing Associate
Gun + Partners, Istanbul

begum.yavuzdogan@gun.av.tr

This article has been published in **e-commerce law and policy**

The online version can be found here