Privacy issues in M&A transactions in Turkey

by Begüm Yavuzdoğan Okumuş, Gün + Partners

Articles | Law stated as at 01-Dec-2018 | Turkey

This article reviews data protection issues in different phases of an M&A transaction in Turkey, and how the parties must plan data transfers during the transaction and be prepared for privacy-related post-closing issues.

The article is part of the global guide to private mergers and acquisitions. For a full list of jurisdictional Q&As visit *global.practicallaw.com/privateacquisitions-guide*

Among other things, privacy issues in mergers and acquisitions now attract the attention of transaction parties.

Privacy risks/issues in mergers and acquisitions used to be overlooked or underestimated. However, these days, conducting adequate due diligence on privacy issues and mitigating risks associated with a target's privacy-related liabilities, as well as requesting privacy-related representations and warranties, are common in merger and acquisition transactions.

The other important issue is how the target company can disclose the required data to the purchaser (and the purchaser's advisers), including personal data and the risk associated with such transfer, and how the purchaser will use such data on closing.

Purchasers now also have to think about further post-closing items to be dealt with in terms of data protection, according to the jurisdiction where the transaction takes place.

This article reviews data protection issues in different phases of the transaction, and how the parties must plan data transfers during the transaction and be prepared for privacy-related post-closing issues.

Data protection issues in M&A

Transferring/disclosing personal data to the purchaser

Merger and acquisition transactions involve the disclosure or transfer of personal data from the target company to a purchaser. The data being transferred generally relates to personal data of employees, customers, users, suppliers or other business partners. Although most of the personal data is fully transferred at closing, some disclosure may also happen during due diligence, or at any stage between signing and closing. A party must ensure that disclosure/transfer of personal data to the purchaser does not violate any privacy rules of applicable law.

Transfer/disclosure of personal data from the target to a purchaser under Turkish law

Under Turkish law, the disclosure of data relating to data subjects must comply with the Turkish Data Protection Law numbered 6698, enacted on 7 April 2016 (Data Protection Law). The Data Protection Law introduces a definition

of personal data, defining it as "any type of information that relates to an identified or identifiable natural person". In this sense, personal data can only relate to natural persons.

Processing of personal data is permitted when it is based on grounds stipulated under the Data Protection Law. Personal data can be processed and transferred to a third party, if one of the following applies:

- The data subject has provided explicit consent.
- The processing is clearly mandated by law.
- For a person who is unable to express their explicit consent, the processing is required for the safeguarding of his/her or a third person's life or physical wellbeing.
- The processing is directly related to the formation or execution of an agreement to which the data subject is a party.
- The processing is required for the data controller to satisfy its legal obligation.
- The data to be processed has been made public by the data subject.
- The processing is mandatory for the establishment, use or protection of a right.
- On 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.

In case of a breach of data protection rules, affected persons can claim damages and seek compensation before courts. Further, in case of an unlawful processing, administrative fines can be imposed due to breaching data safety obligations and enabling unlawful data processing. Breach of data protection rules may under certain circumstances result in criminal liability. Criminal liability does not apply to legal persons but natural persons committing such a crime can be liable.

Can explicit consent be a ground?

In light of the above, in an M&A context, it does not seem practical to rely on the consent of the data subjects, since the contemplated transaction might be confidential until closing takes place. It may also be difficult to follow a consent procedure (which includes providing adequate information to the data subject before obtaining the consent), and consent can be withdrawn at any time. Therefore, consent is only used in practice when very few individuals are involved and they have reason to be aware of the contemplated transaction. Further, consent must be explicit, freely given and based on appropriate information to be held valid.

However, in a transfer of sensitive data, the data subject's consent to the transfer is required and sufficient precautions determined by the Data Protection Authority must be in place.

Can a legitimate interest of the data controller/target company or the purchaser/data recipient be a ground?

Legitimate interest is determined as a last resort ground for data processing. It requires a balance test when applied, and the fundamental rights and liberties of the data subject must be protected. In an M&A transaction, a "legitimate interest" ground can be used. It is in the legitimate interest of the purchaser to receive the relevant data to be able to make an assessment/evaluation of the target company, and also the target company to provide the data to the purchaser so that a correct evaluation can be made. However, this ground has certain limitations, since use of such

data must be proportionate with the purpose, and data that is not needed for such an evaluation before closing must not be transferred.

Alternatively, certain other precautions can be taken to keep personal data confidential or if it cannot keep confidential, such data can be transferred very carefully under conditions and must not be excessive. In practice, it is therefore often advisable to try to wait until all or most of the conditions to closing of the transaction have been satisfied before transferring personal data based on this ground.

Can formation or execution of a contract be a ground?

Formation or execution of a contract with the data subject can be a ground when the transaction includes a transfer of contracts the data subject is party to, and where personal data must be transferred for the contract to be performed.

Even when personal data is transferred based on these grounds, the transfer must be limited to the purpose of data processing, and must not be excessive. For instance, while transferring employee data some aspects of personal data must be deleted, anonymised, and transfer must be limited to personal data necessary for the purchaser to make a valid and correct evaluation.

Risks associated with transfers at closing

At closing, the purchaser will expect to receive all personal data related to the acquired business. Then the data subjects must be informed of the transfer. The seller should give the data subjects certain information about the transfer of their data to a third party.

Data transfers abroad

Additional steps must be taken in a transfer of data outside Turkey. Data rooms are now mostly established as virtual data rooms. It is possible that the server of the online platform is based in a foreign country (with or without an adequate level of protection).

To transfer personal data abroad, the explicit consent of the data subject can be a legal ground. The above legal grounds can also be used if the foreign country has sufficient safeguards to protect personal data. If they do not have such adequate safeguards, the data controller in the foreign country must undertake in writing to the Turkish Data Protection Authority to provide adequate protection for equivalent safeguards and the approval of the Authority must be obtained. Countries that have sufficient safeguards are determined by the Turkish Data Protection Authority. For the time being, the safe country list has not yet been announced.

Therefore, currently, consent of the data subjects will make the transfer of data abroad lawful under Turkish law, but it may be difficult or burdensome.

In the absence of a safe country list issued by the Turkish Data Protection Authority or individual consent obtained from the data subjects, an M&A-related data transfer must therefore only be made after the data controller in the foreign country undertakes to the Turkish Data Protection Authority to provide adequate protection in writing for equivalent safeguards and the approval of the Authority must be obtained. Planning ahead is important, as approval, if needed, may take a long time.

Notification to the Data Controllers' Registry: post-closing

Under Turkish Law, there is a requirement for data controllers to be registered with the Data Controllers' Registry. This is a platform open to the public where data controllers provide information about themselves and record the data categories they process.

The Turkish Data Protection Authority recently announced that the following are exempt from the obligation to register with the Data Controllers Registry:

- Data controllers that process personal data through non-automatic means, provided that the processing is part of a data recording system.
- Public notaries.
- Foundations, associations and unions that only process personal data of their own employees, members and benefactors, provided that the processing is limited to their field of operations and in line with their purposes and the relevant legislation.
- Political parties.
- Attorneys.
- Public accountants.
- Sworn-in public accountants.
- Customs brokers operating under the Customs Law numbered 4458 and authorised customs brokers.
- Mediators.
- Data controllers with less than 50 employees with an annual financial balance sheet of less than TRY25 million, whose field of operations is not the processing of sensitive data.

Further, companies that must register with the Data Controllers' Registry must prepare a data inventory. This includes:

- The purposes of data processing.
- Data categories.
- The data recipients.
- The maximum time periods required for the purposes of processing.
- Data to be transferred abroad.
- Measures to be taken for data security.

Companies residing in Turkey must appoint a contact person responsible for liaising with the Authority. Companies not residing in Turkey must appoint a data controller representative, which is a legal entity or a real person with Turkish citizenship who will be in communication with the Authority, answer requests addressed to the data controller and do things related to the Data Controllers' Registry on behalf of the data controller. All companies must prepare a data preservation and destruction policy.

In light of the above, after closing the target company may become obliged to register with the Data Controllers' Registry or to update the information already provided to the registry (if it is already registered). Changes must be

notified to the Data Controllers' Registry within seven days, so the purchaser will have another post-closing item to deal with.

Post-closing

After closing, the purchaser must consider how to integrate the personal data received from the target and the target's IT systems into its own data and systems. It is important to determine whether the privacy policies of the target and the purchaser are similar, or whether the purchaser's is less protective than the target's.

In addition, the purchaser must inform data subjects about the closing and results of the transaction and the new data processing regime, possibly as part of the information obligation under the Law. Obtaining consent from the data subjects for the transfer of data may be considered, or the purchaser may need to take necessary actions to ensure that the cross-border data transfer is legal.

Summary

Before signing, the purchaser's due diligence must outline all potential risks associated with the target's privacy-related liabilities, and relevant representations in M&A agreements must be in place.

Between signing and closing, both the seller and purchaser must be careful in the disclosure of personal data and manage the disclosure process, to ensure that the transfer of data is limited to the purpose of the processing and not excessive. Further, access to the data room must be strictly limited to those persons who really need to know and assess the documents, and confidentiality agreements must be executed.

After closing of the transaction, the purchaser must consider diligently what steps must be taken to use the acquired data lawfully.

In case closing does not take place and negotiations fail, the persons granted access to the data must agree to destroy all received data including due diligence results, and personal data must receive special attention in such destruction. In practice, access to data is made available upon the participant accepting the confidentiality and data protection rules before accessing the data room.

M&A transactions often involve several jurisdictions. It is essential to manage different applicable data privacy rules in different jurisdictions beforehand, so as not to be exposed to data privacy-related risks and obligations.

Contributor profile

Begüm Yavuzdoğan Okumuş, Managing Associate

Gün + Partners

T +90 212 354 00 24
F +90 212 274 20 95
E *begum.yavuzdogan@gun.av.tr*

W *www.gun.av.tr*

Professional qualifications. Lawyer, Turkey, CIPP/E

Areas of practice. Corporate and M&A; competition; life sciences; technology, media and telecom.

END OF DOCUMENT

