Bill to amend Turkish Data Protection Law is submitted to Parliament

February 2024

A Justice Reform Bill containing provisions to amend important aspects of the Turkish Data Protection Law No. 6698 (DPL) was submitted to the Turkish Parliament on 16 February 2024.

Focusing on restrictions to cross-border data transfers and the processing of sensitive data, the Bill marks a first concrete step towards completing the harmonisation of the DPL with the EU acquis, especially the European Union General Data Protection Regulation (GDPR), as described under the Medium Term Programme (2024-2026) published by the Turkish Strategy and Budget Directorate in September 2023.

The preamble to the Bill underlines that the current situation, especially regarding the transfer of personal data abroad, makes it almost impossible for companies to use cloud-based software and applications with servers located outside Turkey, while these are a common feature in business practice. In this context, the Bill aims to reorganise the conditions surrounding the transfer of personal data abroad and the processing of sensitive data, taking into account current business needs and the GDPR.

Cross-border data transfers

Currently, Turkish law only allows the transfer of personal data abroad with the consent of the data subject or, where an exception to consent applies, either to a country recognised as providing adequate protection or with the prior approval of the Data Protection Authority (DPA) on the basis of standard contractual clauses or binding corporate rules. In practice though, no country has yet been recognised as providing adequate protection, and the DPA has only issued a few decisions authorising cross-border data transfers on the basis of standard clauses. This means that most companies have to rely on the data subjects' consent, which is both impractical and risky, as consent may be invalid if not freely given.

The Bill proposes a complete overhaul of the legal basis to transfer data abroad, which would now be possible in one of the following cases: (i) where the DPA has issued an adequacy decision; (ii) where one of the

appropriate safeguards is in place; or (iii) in other exceptional cases. A separate regulation will be issued regarding the procedures and principles to implement the new framework on cross-border data transfers.

Adequacy decision. The Bill provides that where an exception to consent applies (e.g. the transfer is necessary to comply with a legal obligation or pursue a legitimate interest), personal data can be transferred abroad in the presence of an adequacy decision taken by the DPA with respect to a specific country, international organisation or sector.

The adequacy decision will take into consideration reciprocity, the legislation of the relevant country, the international conventions to which Turkey is a party, and the global or regional organisations of which it is a member. The decision will be re-evaluated every four years at the latest.

While this remains fairly similar to the current system, the Bill introduces a mechanism for more targeted adequacy decisions, which could be limited to a specific organisation or sector. This may make it more feasible for the DPA to issue adequacy decisions in practice.

Appropriate safeguards. Where one of the exceptions to consent applies, the Bill contemplates that personal data can be transferred outside Turkey if one of the following appropriate safeguards is put in place, on the condition that the data subject has the opportunity to exercise their rights and apply for effective legal remedies in the country where the transfer will be made:

(i) agreement between a foreign public institution and a Turkish public institution, with the DPA's prior authorisation to the transfer;

(ii) binding corporate rules approved by the DPA;

(iii) standard contractual clauses entered on the basis of the model published by the DPA, which must be notified to the DPA within five business days of execution; or

(iv) written undertaking containing provisions to ensure adequate protection, with the prior approval of the DPA.

The Bill specifies that these safeguards should also apply to subsequent data transfers carried out abroad.

The most significant development brought by the Bill is the possibility to transfer data abroad on the basis of standard contractual clauses with a mere notification to the DPA, instead of the prior approval process currently in place. The failure to notify the DPA within five business days would be subject to a fine ranging from TRY 50,000 to TRY 1,000,000 (approx. EUR 1,500 to EUR 30,000). The removal of the prior approval process would lift a major practical hurdle for companies, which have had to deal with the uncertainty surrounding the current system, in particular the timeframe within which applications are processed.

Exceptional cases. Under the Bill, where there is no adequacy decision and none of the appropriate safeguards is available, personal data can be transferred abroad in the following exceptional cases, provided that the transfer remains occasional:

(i) the data subject has given explicit consent to the transfer, provided that they have been informed of the possible risks;

(ii) the transfer is mandatory for the performance of a contract between the data subject and the data controller or for the implementation of pre-contractual measures taken at the request of the data subject;

(iii) the transfer is mandatory for the conclusion or performance of a contract between the controller and another natural or legal person for the benefit of the data subject;

(iv) the transfer is mandatory for an overriding public interest;

(v) the transfer is mandatory for the establishment, exercise or protection of a right;

(vi) the transfer is mandatory for the protection of the life or physical integrity of the data subject or another person who is unable to give consent or whose consent is not legally valid; or

(vii) the transfer is made from a registry open to the public or to persons with a legitimate interest, at the request of the person with a legitimate interest and provided that the legal conditions for access to the registry are met.

The above makes it clear that the data subject's consent to the transfer of data abroad should only be obtained in exceptional cases, while it is the main legal tool under the current version of the DPL. If the Bill is adopted as planned, the previous rule would continue to be applied together with the new rules until 1 September 2024.

It is yet unclear how these exceptional cases will be assessed in practice. The Bill makes it a condition that transfers made on these grounds remain occasional. In other words, these grounds can only be used for limited, one-off cases rather than continuous data transfers. The transfer of data necessary to the conclusion or performance of a contract will be of particular interest to companies. Transfers carried out for the purpose of an isolated contract could qualify as exceptional and would not require any additional formality, while others would still be subject to appropriate safeguards, such as standard contractual clauses notified to the DPA. Further guidance will likely be needed through secondary legislation and the decisions of the DPA to clarify the contours of these new exceptions.

Processing of sensitive data

In the current version of the DPL, sensitive personal data other than data relating to health and sexual life can be processed without consent where explicitly contemplated by the law. Data relating to health and sexual life may only be processed without consent (i) by persons under a statutory obligation of confidentiality (such as a workplace doctor) or by authorised institutions, and (ii) for the purpose of protecting public health, preventive medicine, medical diagnosis, treatment and care services, planning and management of health services, or financing of the same.

The Bill proposes to expand the cases in which sensitive data can be processed without obtaining consent from the data subjects. All sensitive data could now be processed without consent where:

(i) it is explicitly stipulated by the law;

(ii) is mandatory for the protection of the life or physical integrity of the data subject or another person who is unable to give consent or whose consent is not legally valid;

(iii) it is related to personal data made public by the data subject of their own free will;

(iv) it is mandatory for the establishment, use or protection of a right;

(v) it is necessary for the protection of public health, preventive medicine, medical diagnosis, treatment and care services, and the planning, management and financing of health services by persons under a confidentiality obligation or authorised institutions;

(vi) it is mandatory for the fulfilment of legal obligations relating to employment, occupational health and safety, social security, social services and social assistance; or

(vii) it is intended for current or former members of foundations, associations and other non-profit organisations or formations established for political, philosophical, religious or trade union purposes,

or for persons who are in regular contact with these organisations and formations, provided that it is in accordance with the legislation to which they are subject and their purposes, limited to their field of activity and not disclosed to third parties.

The Bill is plainly intended to address some of the major loopholes in the current version of the DPL, under which companies were faced with contradictory legal injunctions. In particular, once the Bill is adopted, companies would have a clear legal basis to process sensitive data to comply with their obligations within the scope of the employment relationship or for the purpose of ensuring health and safety in the workplace, without having to obtain explicit consent from their employees.

Judicial challenge to DPA decisions

The current version of the DPL does not contain any provision identifying the competent court to challenge the DPA's decisions. Under general rules of Turkish judicial procedure, a DPA decision imposing a fine on a data controller for breach of the DPL can now be concurrently challenged before the criminal court and the administrative court, albeit on different aspects and subject to different procedures.

The Bill seeks to address this unsatisfactory situation and explicitly sets forth that the fines imposed by the DPA should be challenged before the administrative court. As for the transition period, any case pending before the criminal court as of 1 June 2024 would however continue to be assessed by that court.

The Bill is expected to be discussed in Parliament during the last week of February and to be finalised and adopted in February or March 2024, although the exact timing remains unclear. If the Bill is adopted as planned, the provisions amending the DPL would enter into force as soon as 1 June 2024, subject to limited transitional periods.

Please do not hesitate to contact us for any further information on this briefing.

Contact Us

Stéphanie Beghe Sönmez
Partner
sbeghe@paksoy.av.tr

Mert Karakaşlar
Associate
mkarakaslar@paksoy.av.tr