CIFTCI
ATTORNEY PARTNERSHIP

# AMENDMENTS TO TURKISH DATA PROTECTION LAW

On 2 March 2024, long-awaited amendments to Turkish Data Protection Law were accepted by the Turkish parliament as part of an omnibus bill. The amendments will now await presidential approval, which is expected in the coming days, before entering into force.

The amendments to the Turkish Data Protection Law (Law No. 6698) (the "**TDPL**" – see our previous client briefing on the introduction of the TDPL), principally concern restrictions on the processing of so-called "special categories" of personal data and on transfers of personal data abroad (the "**Amendments**"). They have been accepted by the Grand National Assembly of Türkiye on 2 March 2024, and are planned to enter into force on 1 June 2024 (or 1 September 2024 for international data transfers, allowing a transitionary period of three months).

The Amendments primarily concern overhauling the rules regarding:

- processing of sensitive personal data
- International data transfers

to be less onerous and more closely aligned with the GDPR.

One of the major criticisms of the TDPL has been that its restrictions on international data transfers, which in practice prohibit transfers unless based on explicit data subject consent, give rise to enormous compliance challenges.

## HARMONISATION EFFORTS

The TDPL, which came into effect on 7 April 2016, drew inspiration from the EU's Data Protection Directive 95/46/EC and the Council of Europe's Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data. However, the European legal landscape shifted significantly with the implementation of the EU General Data Protection Regulation (**GDPR**) coming into effect in 2018 after the lapse of its two-year grace period. The GDPR, replacing Directive 95/46/EC, marked the beginning of a global overhaul of data protection standards.

In the wake of the GDPR, Türkiye has been proactive in aligning its data protection framework with international standards. This commitment has now begun to materialise through the inclusion of harmonisation with the EU data protection framework in Türkiye's plans to overhaul parts of its regulatory regime.

It is important to note, however, that the Amendments, unlike changes recently made or proposed to the data protection laws of other countries (for example, India and Switzerland) are primarily aimed at ***harmonisation*** with certain aspects of the GDPR, and reforming some (but not all) requirements of the TDPL which ***go beyond*** the requirements of both Directive 95/46/EC and the GDPR and have posed material compliance challenges in practice, so that they are more closely aligned to the (in these respects) ***less*** onerous EU regime. The TDPL diverges from the GDPR in various other respects which are not addressed by the Amendments.

## THE LAW AS IT STANDS

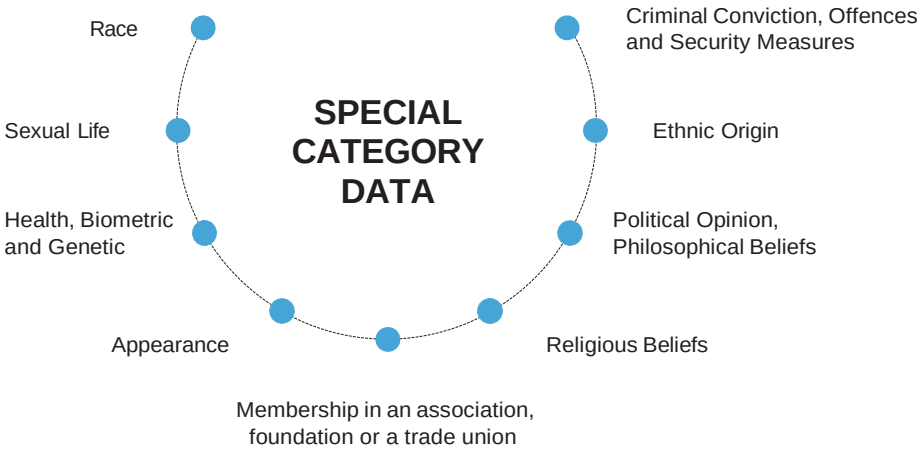
The TDPL already establishes a data protection framework which is broadly consistent with the GDPR regime. In particular, like the GDPR, it:

- regulates the processing of data relating to identified or identifiable natural (but not legal) persons (data subjects);
- is limited in scope to electronic data and data in manual records which are easily searchable by reference to individuals, and excludes processing for purely personal / household purposes;
- distinguishes between "data controllers" (who determine the purposes and means of processing of personal data) and "data processors" (who process personal data on their behalf), with a similar allocation of compliance responsibilities between data controllers and processors;
- sets out a series of high-level principles to be followed in the processing of personal data, based on those in Directive 95/46/EC but broadly similar to those in the GDPR;
- requires all processing of personal data to satisfy at least one of a series of specified lawful bases, which are also similar to those in the GDPR and, in particular, include similarly strict conditions where a data controller relies on ***consent*** to justify processing;
- imposes tighter restrictions on the processing of personal data in certain "special" categories – see below regarding reform of these restrictions;
- requires data controllers to provide data subjects with information about their processing of the data subjects' personal data;
- gives data subjects certain rights – for example, rights to be forgotten and of correction – which they can exercise against data controllers;
- requires data controllers and processors to take steps to keep personal data secure, and to report security breaches to a data protection authority and the data subjects; and
- restricts the international transfer of personal data – see below regarding reform of these restrictions.

## PROCESSING OF SENSITIVE DATA

The TDPL prohibits the processing of personal data in certain special categories unless narrow conditions are met. The GDPR takes a similar approach, but with a somewhat wider range of justifying conditions. The Amendments broaden the circumstances in which special category data can be processed in a manner which broadly reflects the GDPR's (in this respect) more permissive regime and should be helpful in justifying a range of legitimate processing of relatively sensitive data.

Under the TDPL, the special categories cover personal data relating to a data subject's race, ethnic origin, political opinions, philosophical beliefs, religion, religious sect, appearance, or membership of an association, foundation or trade union; health data; data relating to sexual life, criminal convictions, offences or security measures; and biometric and genetic data. This is broadly similar to the categorisation in the GDPR, but diverges from it in four key respects:




- The TDPL extends the GDPR's "trade union membership" category to cover membership of an "association or foundation", which includes associations (*dernek)* and foundations (*vakıf*) that have special status as legal entities under Turkish law.
- The TDPL, unlike the GDPR, includes ***appearance*** as a special category, where appearance might reveal other special categories of personal data (e.g., political opinions, religious beliefs, etc.) – in practice, this may not be significantly broader than the GDPR definition.
- The TDPL treats data relating to ***criminal convictions or security measures*** (and, indeed, relating to criminal offences generally) as special category data. The GDPR prohibits all processing of personal data in this category except where specifically permitted by national law.[1]
- The TDPL does not treat sexual ***orientation*** as special category data.

This categorisation is unaffected by the Amendments.

Under the current law, special category data can only be processed in the following very narrow circumstances:

- with the data subject's explicit consent;
- except for data relating to health or sexual life, where the processing is "*provided for by laws*"; or
- in the case of data relating to health or sexual life, by entities bound by confidentiality obligations or competent public institutions and organisations. This is permissible for purposes such as safeguarding public health, preventive medical operations, medical diagnosis, treatment and nursing services, and the planning, management, and financing of healthcare services.

The first and third of these conditions broadly reflect equivalent conditions in Articles 9(2)(a), (h) and (in part) (i) of the GDPR.

1 Although note that the national law of the UK, for example, which continues to implement the GDPR post-Brexit, treats processing of personal data relating to criminal convictions or security measures in broadly the same way as special category data – this is consistent with, but not actually required by, the GDPR.

The Amendments integrate most of the remaining conditions in Article 9 of the GDPR into the TDPL. Consequently, in addition to the existing available conditions, the processing of special category data will now be permitted if:

- the data are processed for the protection of the vital interests of the data subject or another person (see GDPR Art. 9(2)(c));
- the data have manifestly been made public by the data subject, and the processing is consistent with the intentions of the data subject in making them public (which is more restrictive than GDPR Art. 9(2)(e));
- the processing is for the establishment, exercise or defence of legal claims (GDPR Art. 9(2)(f));
- the processing is necessary for the purposes of carrying out obligations in the field of employment, social security or social protection law (GDPR Art. 9(2)(b)); or
- the processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or other not-for-profit body with a political, philosophical, religious or trade union aim and relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes; and the personal data are not disclosed outside that body without data subject consent (GDPR Art. 9(2)(d)).

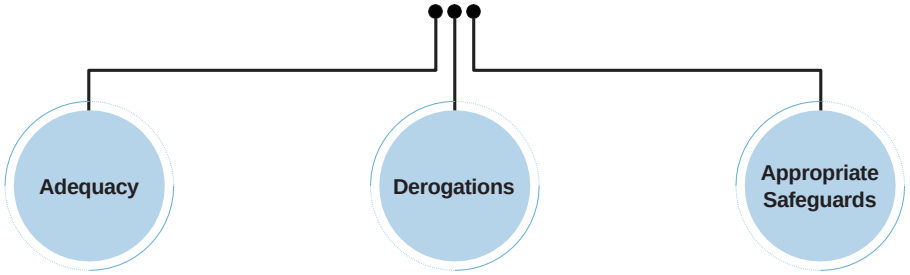
The Amendments do not introduce new conditions for processing of special category data based on substantial public interest (GDPR Art. 9(2)(g)), nor for processing for archiving purposes (GDPR Art. 9(2)(j)). However Article 28 of the TDPL already exempts processing in broadly similar categories from the TDPL's requirements generally, not just from the restrictions on processing of special category data. The public interest exemption is, however, rather narrower than the equivalent condition in the GDPR, at least as it is implemented in some EU member states and the UK.

## INTERNATIONAL DATA TRANSFERS

Currently, the TDPL permits the international transfer of personal data only under specific conditions: (i) explicit consent from the data subject; (ii) an adequacy decision by the data protection authority (**DPA**) in relation to the country to which the transfer is made; or (iii) approval granted by the DPA following an undertaking given by the transferring controller and the recipient outside Türkiye (an **undertaking**).

However, no adequacy decision has yet been reached, despite the TDPL having been in effect since 2016, effectively eliminating one of the legal grounds for such transfers. Furthermore, despite the provision for DPA approval of undertakings, while many applications for approval—more than 80 to date—have been submitted, only a few have received authorisation. In practice, therefore, personal data can only lawfully be transferred outside Türkiye on the basis of explicit consent from data subjects, creating very significant challenges for the legal use of cloud-based software and applications and a wide range of other routine business and other arrangements.

## INTERNATIONAL DATA TRANSFERS




The Amendments create a transfer regime similar to that set out in Chapter 5 of the GDPR, allowing international data transfers to be made, assuming that they comply with the other requirements of the TDPL (e.g. there is a lawful basis for the transfer), provided that:

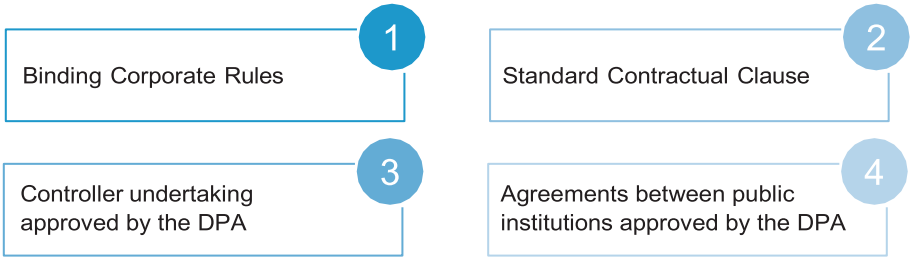
- the DPA has published an adequacy decision in relation to the country to which the transfer is to be made; or
- In the absence of an adequacy decision, appropriate safeguards are provided by the transferring controller or processor.

Appropriate safeguards can (and must) take one of the following forms:

- in the case of intra-group transfers, binding corporate rules in place within a corporate group of companies (**BCRs**) and approved by the DPA;
- an agreement between the exporting data controller or processor and the recipient outside Türkiye which includes standard contractual clauses (**SCCs**) published by the DPA and is notified to the DPA within five business days of its execution;
- an undertaking that is approved the DPA; or
- in the case of transfers made between public institutions or organisations, an agreement (other than an international treaty or convention) between the transferor and the transferee institution or organisation, and the DPA's approval of the transfer.

The available appropriate safeguards therefore include equivalents to all the appropriate safeguards contemplated by Chapter 5 of the GDPR, other than approved codes of conduct and certification mechanisms, which are in practice still at a relatively early stage of development for use under the GDPR. Note, however, that it is not yet clear when or if the DPA will reach adequacy decisions in relation to other countries; and that the DPA has not yet published SCCs, even in draft.

Under the GDPR, the use of approved BCRs or SCCs is not alone sufficient to overcome the Chapter 5 international data transfer restrictions – it is necessary, in addition, for the exporting data controller or processor to conduct a so-called "transfer impact assessment" and satisfy itself that, following the transfer, "*enforceable data subject rights and effective legal remedies for data subjects*" will be available in the transferee jurisdiction in respect of the transferred personal data. At this stage there is no equivalent requirement under the amended TDPL.




Finally, in the absence of an adequacy decision or appropriate safeguards, international data transfers can be made based on a number of conditions that are essentially the same as those in Articles 49(1)(a) to (g) of the GDPR (the **derogations**).
The derogations are:

a. explicit and adequately informed data subject consent;

b. the transfer being necessary for the performance of a contract between the data controller and the data subject;

c. the transfer being necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;

d. the transfer being necessary for important reasons of public interest;

e. the transfer being necessary for the establishment, exercise or defence of legal claims;

f. the transfer being necessary in order to protect the vital interests of the data subject; and

g. the transfer being made from a public register meeting specified criteria; and meeting the conditions for access to the register.

The Amendments explicitly state that transfers relying on the derogations can only be made on an “occasional” basis. The GDPR includes a similar constraint, but only in relation to derogations (b), (c) and (e) (although European data protection authorities have expressed reluctance to accept that the other derogations can be used to justify systematic, bulk or repetitive transfers).

The GDPR includes an additional derogation, permitting certain non-repetitive transfers that concern a limited number of data subjects and are necessary for the compelling legitimate interests of the data controller. There is no equivalent derogation in the Amendments, but this derogation, requiring notification of each transfer to the competent data protection authority, is in any case narrow in scope and, so far as we are aware, rarely relied upon in practice.

## JUDICIAL REVIEW

Under the TDPL, review of administrative fines and sanctions imposed by the DPA is currently within the purview of the criminal courts of peace, a jurisdiction which has been found wanting by the Turkish Constitutional Court. The Constitutional Court has criticised the standard of judicial review by the criminal courts of peace, noting that judgments frequently lack adequate legal reasoning, and do not address the claimants' objections, therefore failing to provide a fair judicial review, due to the courts' high caseload and lack of specialisation. Addressing this, the Amendments specify that the competent courts for such matters will now be administrative courts, aligning with the judicial review process applied to acts of other administrative bodies, such as the competition authority.

## REMAINING DIVERGENCE FROM THE GDPR

As we have discussed, the Amendments for the most part seek to ***reduce*** the compliance burden imposed by the TDPL, in ways that are broadly consistent with the regulatory approach taken by the GDPR. There will remain several respects in which the TDPL diverges from the GDPR, for example:

- The GDPR includes relatively clear and precise provisions setting out its ***territorial scope***. The TDPL is silent on territorial scope, and has been interpreted by the DPA as applying to any processing of personal data within Türkiye, and also to processing of personal of data relating to Turkish citizens or residents which is carried out ***outside*** Türkiye – the claimed extra-territorial application of the TDPL is therefore substantially wider than that of the GDPR.
- The GDPR includes a range of "accountability" requirements, requiring steps to be taken to ensure compliance – for example, requirements to maintain records of processing activities, to conduct impact assessments in relation to high-risk processing, to build "privacy by design" principles into systems and processes, and – in some circumstances – to appoint internal data protection officers, as well as general requirements to implement "appropriate measures" to ensure and be able to demonstrate compliance with the GDPR's principles. None of these requirements has an equivalent in the TDPL, although in many cases the DPA may regard them as best practice in order to ensure compliance.
- The GDPR gives data subjects rights of ***access*** to their personal data, which (with exceptions) they can exercise against data controllers. The TDPL includes only limited rights of ***information***, not extending to access to copies of the actual personal data processed.
- The GDPR intensively regulates relationships between data controllers and processors, for example requiring agreements including a variety of specified provisions to be put in place between them. The TDPL does not impose equivalent requirements.

- The GDPR includes a specific and strict regime applicable to the use of automated decision-making techniques to make significant decisions about data subjects without human intervention – of particular importance with the increasing use of AI applications. The TDPL includes a data subject right to object to the use of such techniques, but in the context of a broadly permissive regime – note that proposed changes to the ***UK*** regime, which may take effect during the course of 2024, would similarly reduce the restrictions on automated decision-making.
- The GDPR allows data protection authorities to impose very substantial sanctions for breach, including fines of up to the greater of EUR 20 million and 4% of an organisation's global annual turnover. The TDPL does include the possibility of substantial administrative fines, but set at a very much lower level (a maximum of TRY 9.4 million for 2024, c. EUR 281 thousand). On the other hand, the TDPL (unlike the GDPR) also creates criminal offences which can be punished by imprisonment.
- The TDPL, like many of the pre-GDPR data protection regimes in the EU, requires data controllers to maintain registrations with the DPA. There is no equivalent requirement in the GDPR, although note that the ***UK*** regime similarly includes what amount to registration requirements.

## CONCLUSION AND NEXT STEPS

The Amendments have been widely welcomed by stakeholders as addressing two major challenges in the Turkish data protection framework. Additionally, the recitals to the Amendments hint at further revisions to the Turkish data protection regime to harmonise more closely with the EU regime.

CIFTCI
ATTORNEY PARTNERSHIP

# AUTHORS

Itir Çiftçi
Managing Partner
Istanbul
T: +90 212339 0 077
E: Itır.ciftci@
ciftcilaw.com.tr

Ekin Öner
Associate
Istanbul
T: +90 212339 0 075
E: ekin.oner@
ciftcilaw.com.tr



www.ciftcilaw.com.tr



Ciftci Attorney Partnership is registered with the Istanbul Bar.

Registered office: Kanyon Ofis Binası Kat 10, Büyükdere Cad. No. 185, 34394 Levent, Istanbul, Türkiye

March 2024

2402-009868