CLOUD COMPUTING

Turkey

LEXOLOGY
Getting The Deal Through

Consulting editor
Bryan Cave Leighton Paisner (BLP)

Cloud Computing

Consulting editors

Marcus Pearl

Bryan Cave Leighton Paisner (BLP)

Quick reference guide enabling side-by-side comparison of insights into local markets; policy and incentives; legislation and regulation; data protection and privacy considerations; typical forms of contract and contractual terms; taxation; and recent notable cases, decisions and trends.

Generated 22 November 2021

Table of contents

MARKET OVERVIEW

Kinds of transaction

Active global providers

Active local providers

Market size

Impact studies

POLICY

Encouragement of cloud computing

Incentives

LEGISLATION AND REGULATION

Recognition of concept

Governing legislation

Breach of laws

Consumer protection measures

Sector-specific legislation

Insolvency laws

DATA PROTECTION/PRIVACY LEGISLATION AND REGULATION

Principal applicable legislation

CLOUD COMPUTING CONTRACTS

Types of contract

Typical terms for governing law

Typical terms of service

Typical terms covering data protection

Typical terms covering liability

Typical terms covering IP rights

Typical terms covering termination

Employment law considerations

TAXATION

Applicable tax rules

Indirect taxes

RECENT CASES

Notable cases

UPDATE AND TRENDS

Key developments of the past year

Contributors

Turkey

Sinem Mermer
smermer@boden-law.com
Boden Law

BODEN LAW

MARKET OVERVIEW

Kinds of transaction

What kinds of cloud computing transactions take place in your jurisdiction?

Following the global trend, there has been an increase in the demand for cloud computing services in Turkey. All three generally known types of cloud services are available: software as a service (SaaS), infrastructure as a service (IaaS) and platform as a service (PaaS) and service providers offer all deployment models: public, community, private and hybrid cloud. In 2021, Turkcell, a leading telecommunications company, announced that a data centre established in Ankara dedicated only to the public authorities, will provide private cloud services.

Active global providers

Who are the global international cloud providers active in your jurisdiction?

Turkey's Informatics Industry Association published a report on the ICT sector's market data and trends for 2020 (Report). According to the Report, 49 per cent of the participants predicted that cloud computing would be the most transforming technology in their sector for the following year. (This number was 70 per cent in 2019.) The Report states that the ratio of companies operating in cloud computing out of all participant companies and the share of cloud computing in their overall turnover was stable compared to the previous year. Forty per cent of the participants reported that a cloud computing product or service is included in their annual turnover 2020. The turnover gained from cloud products or services compared to the total turnover was 12 per cent. Although the Report does not indicate the size of the cloud computing market in Turkey, the total ICT market size was set at US$26.9 billion. Moreover, the International Data Corporation Turkey expected a compound growth rate of 16.1 per cent for the Turkish cloud market between 2017 and 2021. The headquarters of CloudTalk Global, the largest Cloud tech event in Eurasia, is located in Istanbul. The conference and expo were held in Istanbul in 2020 with participants from 15 different countries, and the online event held in 2021 welcomed more than 2,000 participants from 20+ different countries.

Active local providers

Name the local cloud providers established and active in your jurisdiction. What cloud services do they provide?

Research conducted by the Turkish Statistical Institute on the use of information technologies revealed that 40.8 per cent of undertakings with 250 employees and more used paid cloud computing services in 2020. The same data showed that the use of paid cloud computing services in undertakings with less than 250 employees has increased by an average of 4.3 per cent compared to 2018.

Market size

How well established is cloud computing? What is the size of the cloud computing market in your jurisdiction?

Turkey's Informatics Industry Association published a report on the ICT sector's market data and trends for 2020 (Report). According to the Report, 49 per cent of the participants predicted that cloud computing would be the most transforming technology in their sector for the following year. (This number was 70 per cent in 2019.) The Report states that the ratio of companies operating in cloud computing out of all participant companies and the share of cloud

computing in their overall turnover was stable compared to the previous year. Forty per cent of the participants reported that a cloud computing product or service is included in their annual turnover 2020. The turnover gained from cloud products or services compared to the total turnover was 12 per cent. Although the Report does not indicate the size of the cloud computing market in Turkey, the total ICT market size was set at US$26.9 billion. Moreover, the International Data Corporation Turkey expected a compound growth rate of 16.1 per cent for the Turkish cloud market between 2017 and 2021. The headquarters of CloudTalk Global, the largest Cloud tech event in Eurasia, is located in Istanbul. The conference and expo were held in Istanbul in 2020 with participants from 15 different countries, and the online event held in 2021 welcomed more than 2,000 participants from 20+ different countries.

Impact studies

Are data and studies on the impact of cloud computing in your jurisdiction publicly available?

Research conducted by the Turkish Statistical Institute on the use of information technologies revealed that 40.8 per cent of undertakings with 250 employees and more used paid cloud computing services in 2020. The same data showed that the use of paid cloud computing services in undertakings with less than 250 employees has increased by an average of 4.3 per cent compared to 2018.

POLICY

Encouragement of cloud computing

Does government policy encourage the development of your jurisdiction as a cloud computing centre for the domestic market or to provide cloud services to foreign customers?

The Information and Communication Technologies Authority (ICTA) published a Strategic Plan for 2019–2023. One of the policies involved in The Strategic Plan is to utilise information technologies, especially for SMEs, and enact necessary administrative and legal regulations to expand cloud services. The Strategic Plan aims to raise awareness and enhance information security mechanisms to develop cloud computing services. The 11th Development Plan on ICT places cloud computing in the centre of digital transformation. The Turkish Employment Agency has training programmes in order to increase the number of cloud computing specialists.

Incentives

Are there fiscal or customs incentives, development grants or other government incentives to promote cloud computing operations in your jurisdiction?

The Scientific and Technological Research Council of Turkey (TUBITAK) provides funds and scholarships for cloud computing projects and research. Additionally, there are ongoing public, private and EU projects within TUBITAK's Cloud Computing and Big Data Research Laboratory (B3LAB). B3LAB also aims to encourage the growth of qualified researchers to provide training and consultancy to the concerned institutions.

LEGISLATION AND REGULATION

Recognition of concept

Is cloud computing specifically recognised and provided for in your legal system? If so, how?

There is no legal definition of cloud computing technologies. Yet, there are references to cloud computing technologies

or services within the scopes of personal data protection, data localisation and cybersecurity for public institutions and companies operating in certain sectors such as finance, energy and electronic communications.

Governing legislation

Does legislation or regulation directly and specifically prohibit, restrict or otherwise govern cloud computing, in or outside your jurisdiction?

Presidential Circular No. 2019/12 (Circular), published and entered into force on 6 July 2019, sets out information and communications security measures to be applied by public institutions, public organisations and undertakings providing critical infrastructure services. Critical infrastructure sectors are energy, electronic communications, banking and finance, transportation, water management and critical public services (eg, national security, healthcare). As per the Circular, public institutions and organisations shall not store their data in cloud storage services except for their own private systems or local service providers controlled by the institutions themselves. It is also mentioned in the Circular that all email data servers of public institutions should be located in Turkey, although there is no specific reference to cloud computing systems. Relying on the Circular, Digital Transformation Office at the Presidency (DTO) published its Information and Communication Security Guide (Guide) in July 2020. DTO explains that provisions of the Circular aim for data localisation. In other words, as long as the data is stored in local data centres and the mentioned security measures are taken, the Circular does not ban local or foreign providers from providing cloud computing services. The Guide contains general security measures and audit specifications for the provision of cloud computing services which are binding for the public institutions and any other companies operating in critical infrastructure sectors.

Additionally, there are directly applicable sector-specific provisions regarding cloud computing in Turkish law. These are as follows:

- As per the Regulation on the Information Systems of Banks and Electronic Banking Services, banks can use private cloud computing services for their information systems. However, the use of community cloud services is subject to obtaining permission from the Banking Regulation and Supervision Agency (BRSA).
- Financial leasing companies, factoring companies and financing companies incorporated in Turkey may use private cloud services for their information systems. These companies may use community cloud services only after obtaining permission from BRSA.
- As per the Regulation on the Management and Audit of Information Systems of Payment and Electronic Money Institutions, payment and e-money institutions can only process personal data and sensitive payment data through private cloud systems. Nevertheless, these institutions may use cloud computing technologies to process, store and transfer all other data regardless of their deployment method.
- Capital market regulations prohibit data storage institutions from using cloud computing services concerning the data reported to them due to statutory requirements.
- As per the Regulation on Websites to be Operated by Stock Corporations, companies and central database service providers may use cloud computing services outside Turkey.

What legislation or regulation may indirectly prohibit, restrict or otherwise govern cloud computing, in or outside your jurisdiction?

Indirect prohibition or restrictions can be found in the legislations generally in the form of data localisation requirements. Examples are as follows:

- The Law on Regulation of Publications on the Internet and Prevention of Crimes Committed by Means of Such Publication numbered 5651 requires social network providers that track over 1 million daily users from Turkey to implement the necessary measures on hosting the data of users located in Turkey within the country.
- As per the Regulation on Electronic Scooters, operators of shared e-scooter providers are required to locate their servers within Turkey to obtain a licence.
- Publicly listed companies and banks are required to maintain their primary and secondary information systems in the country as per the Communique on the Management of Information Systems, the Regulation on the Information Systems of Banks and Electronic Banking Services and the Regulation on Banks' Internal Systems and Internal Capital Adequacy Assessment Process.
- Payment institutions and electronic money institutions shall keep the documents and logs referred to in the Law domestically for at least 10 years pursuant to the Law on Payment and Securities Settlement Systems, Payment Services and Electronic Money Institutions No. 6493.

Breach of laws

What are the consequences for breach of the laws directly or indirectly prohibiting, restricting or otherwise governing cloud computing?

State officials responsible for implementing the Circular and Information and Communication Security Guide measures may face a judiciary or an administrative disciplinary proceeding due to non-compliance.

The Personal Data Protection Authority is authorised to impose administrative fines to companies in breach of personal data protection legislation.

The Ministry of Trade is authorised to enforce administrative fines to companies violating consumer protection measures.

Consumer protection measures

What consumer protection measures apply to cloud computing in your jurisdiction?

Since there are no consumer protection measures specific to cloud computing, general consumer protection measures would apply to cloud computing products and services. The Law No. 6563 on Regulating Electronic Commerce and the Law No. 6502 on Consumer Protection regulate contracts with consumers that are formed and concluded electronically (distance contracts). Service providers are obliged to provide certain information to consumers before concluding contracts electronically. Among others, consumers must be informed on any technical safeguards that might affect the functionality of the digital software or application. Additionally, service providers are required to ensure that the consumer has the technical means for identifying and correcting input errors prior to the placing of the order and access to contract terms. Distance contracts also shall entail certain rights in favour of consumers, such as the consumer's right of withdrawal from the contract within 14 days following the delivery of services without giving any grounds and paying any fines. If the provider fails to inform the consumers of their right of withdrawal, consumers can exercise their right of withdrawal in one year following the expiration of 14 days. Service providers shall store the electronic logs regarding electronic commerce transactions for three years following the transaction date and submit these logs to the Ministry of Trade upon request. Finally, as per International Private and Procedure Law No. 5718, Turkish Courts at the consumer's residence have jurisdiction if any claims are brought against the consumer. When the consumer files a claim against the service provider, Turkish courts in places where the consumer's domicile or ordinary residence or the other party's domicile or ordinary residence is located are competent. Parties have the freedom to decide on the applicable law subject to the mandatory provisions of the law at the consumer's ordinary residence.

Sector-specific legislation

Describe any sector-specific legislation or regulation that applies to cloud computing transactions in your jurisdiction.

There are several provisions regarding cloud computing in sector-specific legislation such as:

- As per the Regulation on the Information Systems of Banks and Electronic Banking Services, banks can use private cloud computing services for the information systems. However, the use of community cloud services is subject to obtaining permission from the BRSA.
- Financial leasing companies, factoring companies and financing companies incorporated in Turkey may use private cloud services for the information systems. These companies may use community cloud services only after obtaining permission from BRSA.
- As per the Regulation on the Management and Audit of Information Systems of Payment and Electronic Money Institutions, payment and e-money institutions can only process personal data and sensitive payment data through private cloud systems. Nevertheless, these institutions may use cloud computing technologies, regardless of their deployment method, to process, store and transfer all other data.
- Capital market regulations prohibit the use of cloud computing services of data storage institutions concerning the data reported to them due to statutory requirements.
- As per the Regulation on Websites to be Operated by Stock Corporations, companies and central database service providers may use cloud computing services outside Turkey.

Insolvency laws

Outline the insolvency laws that apply generally or specifically in relation to cloud computing.

Turkey does not have specific insolvency laws applicable to cloud computing transactions. Enforcement and Bankruptcy Law No. 2004 (EBL) would be applicable to cloud computing suppliers as well... The EBL contains no explicit prohibition with regards to contractual early termination or automatic termination clauses based on insolvency-related events (except for concord situation). Yet, it is also generally accepted under Turkish law that the bankruptcy administration has a cherry picking right, so that it can cherry pick certain non-monetary obligations and demand their performance. Since it is not clear how customers can obtain their data back from an insolvent cloud computing provider's server, they are advised to opt for contractual measures to mitigate their risk. Reflecting on this risk, cloud computing contracts usually allow parties to immediately terminate the contract if either party becomes insolvent. In some instances, the cloud computing provider may be obliged to transfer the customer's data to another provider immediately when its credit rating is withdrawn or downgraded, or it does not fulfil financial requirements or when there is a decline in its tangible net worth. Customers can also buy services from multiple providers or have back-up servers to avoid a single point of failure.

DATA PROTECTION/PRIVACY LEGISLATION AND REGULATION

Principal applicable legislation

Identify the principal data protection or privacy legislation applicable to cloud computing in your jurisdiction.

Personal Data Protection Law No. 6698 (that entered into force on 7 April 2016 covers personal data processing

activities in Turkey, including cloud computing.

CLOUD COMPUTING CONTRACTS

Types of contract

What forms of cloud computing contract are usually adopted in your jurisdiction, including cloud provider supply chains (if applicable)?

B2C and B2B cloud computing contracts are frequently concluded in Turkey and can be in different types depending on the provider, offerings, and customer. B2C cloud computing contracts are usually non-negotiable and include boilerplate clauses where consumers accept such contracts via click wrap. B2B cloud computing contracts are negotiable depending on the bargaining power and the types of cloud computing services offered. It is also custom that cloud computing contracts contain links to certain documents (eg, general terms and conditions, service level agreements (SLAs), user policy) that can be amended by the provider unilaterally. Cloud provider supply chains are also common in Turkey where the developers customise the cloud computing services to the customers' needs. With the enactment of the Personal Data Protection Law No. 6698 (PDPL), it has become more common the service providers to include data protection clauses in line with the local law.

Typical terms for governing law

What are the typical terms of a B2B public cloud computing contract in your jurisdiction covering governing law, jurisdiction, enforceability and cross-border issues, and dispute resolution?

In B2B public cloud computing contracts, the law of the provider's principal place of business or place of establishment is usually chosen. In most cases, any disputes arising from the cloud computing contracts are resolved by the local courts at the place that is selected as governing law. Arbitral clauses are rarely incorporated into B2B public cloud computing contracts and the arbitrability of certain aspects of cloud computing contracts (such as data privacy) is subject to judicial review.

In most cases, cross-border issues arise within the scope of data privacy. B2B public cloud contracts may include clauses authorising the provider to process data in a country other than the customer's place of business. Clauses incorporated into the B2B public cloud contracts allow the cross-border transfer of personal data to the extent permissible by the applicable law. That said, the PDPL allows the cross-border transfer of personal data under certain circumstances. Similar to the GDPR, the PDPL permits cross border data transfers to countries with adequate protection in principle. However, the Board has not published its list of countries with adequate protection as of writing. The PDPL sets out two additional methods to be followed for cross-border transfers; both require the Board's authorisation, which are namely commitment letters (or undertaking letters) and binding corporate rules applications. Some B2B public cloud computing contracts also allow providers to use standard contractual clauses for cross-border transfers, which are not regulated in the PDPL. Instead, the PDPL only authorises cross-border data transfer provided that (1) data subjects explicitly consent to the cross-border transfer or (2) the Board approves the commitment letter application.

Typical terms of service

What are the typical terms of a B2B public cloud computing contract in your jurisdiction covering material terms, such as commercial terms of service and acceptable use, and variation?

Commercial terms

It is common that cloud computing contracts include clauses on price and payment. Subscription-based fees are typically included either as flexible (pay-as-you-go) or annual fixed term. The service providers usually invoice the fees on a monthly basis. Usually, service providers reserve their right to change their prices unless indicated otherwise. Overdue payments typically result in the suspension of services.

Acceptable use policy

Most contracts refer to service providers' acceptable use policies, which can be revised from time to time. Acceptable use policies (AUPs) usually contain restrictions to the use of services such as generating unsolicited bulk commercial emails, any unlawful, invasive, defamatory or fraudulent purposes, intentionally distributing viruses, etc, reselling services to third parties. Such policies tend to retain broad and catch-all phrases. In the case of violations to AUPs, service providers usually first notify the consumer and request rectification. If the breach is not corrected, the service provider may suspend or terminate the services.

Variations

Typically service providers reserve their rights to change the policies or services. In the case of substantial changes to terms or services, service providers usually inform the customers of such changes before entering into force.

Typical terms covering data protection

What are the typical terms of a B2B public cloud computing contract in your jurisdiction covering data and confidentiality considerations?

In B2B public cloud computing systems, it is common that service providers retain provisions allowing them the utmost flexibility in data protection within the borders of applicable law. Local service providers are more inclined to include provisions that would restrict the service providers' actions in data transfers, security levels, etc.

Data security

Typically cloud computing contracts include clauses on data security stipulating that the service provider would not access or use customer data unless it is required by the law or it is necessary for providing services. It is standard for service providers to indicate that they take all technical and organisational measures to protect personal data. Customers usually have a right to audit by appointing a third-party auditor to inspect the security of data, however, it is advised that customers indicate standards of security in the contract (eg, ISO 27001, ISO 27018).

Data integrity and preservation

Cloud computing contracts usually state that customers' data remain complete and valid. To achieve data integrity, cloud providers offer security walls, anti-virus protections, back-up and recovery services, penetration tests, etc. In terms of data preservation, contracts may include measures to be taken by the service provider in the case of accidental loss, unauthorised erasure of data. Such measures include, inter alia, back-up systems, uninterruptible power supplies in data centres and testing of emergency systems.

Location of servers and data or cross-border transfers

Standard terms of cloud computing contracts usually do not contain provisions on the location of servers but rather indicate that customer data can be stored and processed in any country that the service providers maintain facilities. Depending on the sector and the bargaining power, customers usually request to insert clauses restricting the cross-border transfers or determining location of servers. Due to the restrictions to cross-border transfer of personal data and sector-specific rules regarding data localisation, service providers offer specific cloud computing services to accommodate such needs.

Data disclosure and confidentiality (general)

In most cases, the confidentiality provisions are mutual. Confidentiality provisions generally include a definition of confidential information, level of protection and exemptions. These clauses apply to all confidential information exchanged before and during the contract term. Data disclosure is usually allowed only to agents or employees on a need-to-know basis or if required by law (court order, decision of governmental authorities).

Typical terms covering liability

What are the typical terms of a B2B public cloud computing contract in your jurisdiction covering liability, warranties and provision of service?

Warranties

Generally, both parties warrant that they have the legal capacity to conclude the cloud computing contract, and they would act in compliance with all applicable laws and rules on the provision and use of services. In some contracts, service providers also warrant services to be in line with the contractual documents, and they would use reasonable care expected from other (global or local) service providers. In clickwrap cloud computing contracts, it is common that customers are liable for integrity and preservation of their data; thus, contracts do not contain warranty clauses in this regard. Most contracts contain a boilerplate disclaimer provision stating that no other warranties are provided to the customers except as expressly provided therein.

Limitation of liability

Limitation of liability clauses vary depending on the offering and customer. Most commonly, service providers exclude any indirect liability, including inter alia loss of profit, punitive damages, penalties, loss of reputation. Usually, liabilities are capped with the annual subscription fees. Exclusion and cap on liability are mutual in some contracts. Occasionally, service providers expressly exclude all liability if cloud services are offered for free. Commonly, cloud contracts do not limit liabilities if the obligations are breached: indemnifications, confidentiality obligations, data protection and security obligations due to unauthorised use or disclosure of data, damages arising from gross negligence or wilful conduct or payment obligations.

Indemnification

Generally, the scope of indemnifications varies widely. Indemnification clauses set forth that service providers will defend the customers (and in some cases its affiliates) in any proceeding arising from an allegation that the offerings infringe a third party's IP rights or disclosure of trade secrets, and customers shall defend service providers in any proceeding arising from customer data or a breach of acceptable use policy. Indemnification obligations are

sometimes exempted under certain circumstances, such as infringements arising from indemnified party's breach. Indemnification can also be subjected to written notification of allegations to the other party or allowing the party to appoint its representative who also has an obligation to defend itself.

Service-level agreements and system availability

Some cloud computing contracts entail clauses or refer to a separate service level agreement (SLA) on system availability. Service providers sometimes guarantee a minimum percentage of system availability calculated based on total use time and downtime each month. In some cases, service providers provide credits to customers if the determined rate is not reached. Occasionally, credits can be deducted from the subscription fees. Typically, service providers request customers to notify if such rates are not achieved, whereas customers wish the service providers to monitor and notify. In rare cases and upon the customers' request, the contract may be terminated by the customer if the system availability rate is not reached within a defined period. Moreover, SLAs usually determine the incident response times, backup and restoration measures.

Typical terms covering IP rights

What are the typical terms of a B2B public cloud computing contract in your jurisdiction covering intellectual property rights (IPR) ownership in content and the consequences of infringement of third-party rights?

Commonly, cloud computing contracts expressly state that customers own IP rights of their data and service providers own IP rights of their services. Service providers usually reserve their right to access or use customer data to the extent necessary for providing its cloud computing or professional services while taking measures to protect customer data. Indemnification clauses typically refer to the infringement of third-party IP rights. Such clauses usually state that service providers indemnify, defend and hold customers harmless if an allegation arises from IP infringements.

Typical terms covering termination

What are the typical terms of a B2B public cloud computing contract in your jurisdiction covering termination?

Cloud computing contracts can be terminated immediately by either party if the other party materially breaches the contract and fails to cure the breach within the defined period or if one party becomes insolvent or ceases its operations. In rare cases, customers do not have the right to terminate the contract for convenience. Upon the effective date of termination, customers do not have access to the services, and all unpaid due fees are to be paid to service providers. Rarely, service providers are obliged to refund fees depending on the terms of the contract. Usually, service providers define a period (eg, 180 days) for customers to migrate their data before denying access to the services.

Employment law considerations

Identify any labour and employment law considerations that apply specifically to cloud computing in your jurisdiction.

Cloud computing contracts typically contain no agency clauses stating that the contract does not establish any agency, partnership or joint venture between the parties. On the other hand, retaining cloud computing services can be defined as outsourcing as per the Labour Law and the Regulation on Subcontractors. These regulations differentiate

outsourcing a part of main operations or auxiliary works that will be determined according to the customers' field of activity. If retaining cloud computing services is to be deemed outsourcing, mandatory rules arising from the applicable law (eg, mandatory provisions to be inserted to the outsourcing contract) should be abided by. To the best of our knowledge, this issue has not been subjected to judicial review yet.

TAXATION

Applicable tax rules

Outline the taxation rules that apply to the establishment and operation of cloud computing companies in your jurisdiction.

There are no particular taxation rules applicable to cloud computing companies. Overall, corporations are taxed based on whether their legal or business centre is located in Turkey or not. Those who have their legal or business centre in Turkey are defined as taxpayers with full liability, whereas those with neither their legal nor business centre in Turkey are defined as taxpayers with limited liability. Full taxpayers are taxed based on the revenues they generate globally, whereas limited taxpayers are taxed based only on the revenue they generate from Turkey. Therefore, establishing what constitutes a business centre is the key question that will be evaluated as per the Turkish tax law and the relevant bilateral agreements for the avoidance of double taxation, if applicable.

Indirect taxes

Outline the indirect taxes imposed in your jurisdiction that apply to the provision from within, or importing of cloud computing services from outside, your jurisdiction.

All services that are performed or their benefits are consumed in Turkey would be subject to VAT. All companies incorporated in Turkey or having a residence, business place, legal centre, or business centre in Turkey are liable for VAT payment. As per article 9 of the VAT Law, the sale of online products by those who do not have a residence, workplace, legal centre, or business centre in Turkey is subject to VAT as long as the services are provided electronically to natural persons who are not VAT payers in Turkey. In this case, VAT will be paid by the companies providing the service. Such corporations need to register to the Revenue Administration through the Special VAT Registration for E-Service Providers which is available at https://digitalservice.gib.gov.tr/ . In the case of B2B sales, these corporations still need to fill out the VAT declaration, yet the buyer would pay VAT (ie, reverse charge mechanism).

Effective from March 2020, sale of any audio, visual or digital content on digital platforms (including computer programs, applications, music, video, games, in-app purchases and other similar products) and digital services offered to listen, watch, play or record these contents in electronic media or use them in electronic devices are subject to digital services tax set at 7.5 per cent. The tax is calculated based on the revenue generated from Turkey. Digital services tax applies to all persons generating revenue from Turkey without making any distinction between a full or limited taxpayer status, save from certain exemptions listed in the Law numbered 7194 on Digital Services Tax.

Both VAT and Digital Services Tax apply to domestic online sales.

In addition to the aforementioned taxes, stamp duty may be applicable in some instances. In accordance with the General Communique on Stamp Tax Law (Serie No: 60), any agreement concluded via an online platform would be subject to stamp duty if it is concluded via electronic signature subject to certain exceptions.

RECENT CASES

Notable cases

Identify and give details of any notable cases, or commercial, private, administrative or regulatory determinations within the past three years in your jurisdiction that have directly involved cloud computing as a business model.

At the beginning of 2021, a holding company operating in multiple sectors filed a lawsuit against Microsoft alleging that the cloud service provider forced the company to transfer its data outside of Turkey. This lawsuit is currently ongoing, and no decision has been published yet. In another commercial dispute, a first instance court ruled that the respondent failed to submit its commercial books even though the respondent argued that its cloud provider restricted its access to company emails and other bookkeeping applications. The first instance court dismissed the defendant's excuse on the grounds that the defendant's relationship with the cloud provider is a separate matter that is to be resolved by the respondent and considered only the evidence brought by the claimant.

UPDATE AND TRENDS

Key developments of the past year

What are the main challenges facing cloud computing within, from or to your jurisdiction? Are there any draft laws or legislative initiatives specific to cloud computing that are being developed or are contemplated?

The covid-19 pandemic has led to an increase in cloud computing investments in Turkey. That being said, currency fluctuations and lack of clarity in data localisation provisions appear to be the main challenges against the development of cloud computing services. In April 2021, the Turkish Presidency published the Human Rights Action Plan, which stated that the Personal Data Protection Law will be revised in line with the standards of the European Union within a year. Therefore, the cross-border transfer scheme may become simplified and compliant with the General Data Protection Regulation.

The author would like to thank Ms Merve Topkoru, legal intern at Boden Law, for kindly assisting in the preparations of this contribution.

Jurisdictions

Austria	MGLP Rechtsanwälte | Attorneys-at-Law
Brazil	Pinheiro Neto Advogados
France	Latham & Watkins LLP
Germany	Greenberg Traurig LLP
Japan	Iwata Godo
Sweden	Advokatfirman Delphi
Switzerland	Kellerhals Carrard
Turkey	Boden Law
United Kingdom	Bryan Cave Leighton Paisner LLP
USA	Bryan Cave Leighton Paisner LLP