Do Turkish Companies Have to Comply With the California Consumer Privacy Act ("CCPA")?

7 January 2020

Authors: **Selin Kaledelen, Damla Çay, Lidya Ercan, Steven R. Chabinsky, F. Paul Pittman**

Your business complies with the General Data Protection Regulation ("**GDPR**") and/or Turkish Personal Data Protection Law numbered 6698 and its secondary legislation ("**PDPL**"); but does it comply with the California Consumer Privacy Act ("**CCPA**"), which took effect on January 1, 2020? If your company needs to comply with the CCPA, some crucial differences should be taken into account in privacy compliance management.

Many businesses are in the process of complying with the GDPR and/or the PDPL; however, some of these businesses might need to comply with the CCPA, as well. When exactly would that be necessary? Compliance with the CCPA might especially be triggered for Turkish businesses providing cross-border services directly to California residents, such as E-commerce, gaming, streaming or payment services. In substance, if a Turkish business is doing business in the State of California and collects the personal information of a person residing in the State of California; it might need to comply with the CCPA, irrespective of the location of its main place of business. While the CCPA is not explicit as to the meaning of "doing business in the State of California", it can be interpreted by a reference to "consumer" and thus, any business collecting and/or selling information of California residents can be considered as "doing business in the State of California". A Turkish business may be subject to the CCPA if it meets any of the following criteria: (i) has annual gross revenue over USD 25,000,000, (ii) annually buys, sells, receives or shares for commercial purposes, the personal information of 50,000 or more consumers, devices or households, or (iii) derives 50 percent or more of their annual revenue from selling consumers' personal information.

Moreover, CCPA, GDPR and PDPL differ in terms of several concepts and scope of application. Therefore, if a Turkish business wishes to comply with the CCPA, it is important to know these differences. Hence, we have prepared the table below to demonstrate some of these differences. In order to get detailed information on the application of the CCPA, please refer to our client alert.

CCPA	GDPR	PDPL	Comments
Issue: Scope: Covered Information and Individuals			
Information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household is "**Personal Information**". Including but not limited to the following: • Identifiers such as a real name, alias, signature, physical characteristics or description, telephone number, postal address, unique personal identifier, online identifier Internet Protocol address, email address, account name, social security number, passport number, driver's license or state identification card number or other similar identifiers, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information. • Characteristics of protected classifications under California or federal law (for example, race, color, sex, age, religion, national origin, disability, citizenship status, and genetic information). • Commercial information, including records of personal property, products or	"**Personal Data**" meaning information relating to an identified or identifiable natural person ('data subject'). An "identifiable natural person" is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Personal data under the GDPR covers publicly available data.	"**Personal Data**" means all the information relating to an identified or identifiable natural person ('data subject'). The PDPL does not specify publicly available data under personal data. However, processing of a data which made publicly available by the data subject might be out of scope.	Organizations that are subject to CCPA and PDPL may see certain nuanced differences between the data about California residents that qualifies as "personal information" for the purposes of the CCPA and data that is "personal data" for the purposes of the PDPL (and the GDPR). Consequently they may, for the purposes of compliance, either closely scrutinize such differences or take a "highest common denominator" approach.

CCPA	GDPR	PDPL	Comments
services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies. • Biometric information. • Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an Internet Website, application, or advertisement. • Geolocation data. • Audio, electronic, visual, thermal, olfactory, or similar information. • Professional or employment-related information. • Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act. • Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities and aptitudes. "Publicly available" information is not included			

CCPA	GDPR	PDPL	Comments
under “personal information”. Information that is lawfully made available from federal, state or local government records; however, if the information is used for a purpose that is not compatible with the purposes for which it is maintained and made available in the government records for which it is publicly maintained, such information is not publicly available. “Consumer” means a natural person who is a California resident….however identified, including by any unique identifier.			
Issue: Scope: Covered Entities			
A “business,” means a for-profit legal entity (or sole proprietorship) collecting personal information about consumers that: • either alone or jointly with others, determines the purpose and means of the processing of consumers’ personal information; and • does business in the State of California; and either A. has annual gross revenue over $25,000,000; B. annually buys, sells, receives or shares for commercial purposes, the personal information of 50,000 or more consumers, devices or households; or C. derives 50 percent or more of their	Anyone who, as a controller or processor: • processes personal data in the context of an EU establishment (whether or not the processing takes place in the EU); or • without having an EU establishment, processes personal data of data subjects in the EU in relation to offering them goods or services, or monitoring their behavior. “Controller” means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. “Processor” means a natural or legal person, public authority, agency or other body, which processes	There is no territorial scope determined by the PDPL, so it would apply to the data controllers or processors collect or transfer data from Turkey. “Controller” means the natural or legal person who determines the purpose and means of processing personal data and is responsible for establishing and managing the data registry system. “Processor” means the natural or legal person who processes personal data on behalf of the controller upon his authorization. “Processing of personal data” means any operation performed upon personal data such as collection, recording, storage, retention, alteration, re-organization, disclosure, transferring, taking over, making retrievable, classification or preventing the use thereof, fully or partially through	The CCPA is narrower than the GDPR and the PDPL in a number of respects here; it applies only to entities that: • are what would be referred to under the GDPR and PDPL as "controllers", and in fact the CCPA closely follows the language used in the GDPR's definition of "controller" and "processing." • do business in California (unless every aspect of the entity's commercial conduct takes place wholly outside of California), whereas the GDPR applies both: to processing taking place outside the EU (where the entity processes personal data in the context of an EU establishment) and to businesses with no EU establishment that are processing personal data about data subjects in the EU. The PDPL applies the entities collect or

CCPA	GDPR	PDPL	Comments
annual revenue from selling consumers' personal information. "Processing" means any operation or set of operations that are performed on personal data [sic] or on sets of personal data, whether or not by automated means.	personal data on behalf of the controller. "Processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means.	automatic means or provided that the process is a part of any data registry system, through non-automatic means.	transfer data from Turkey. • exceed one of the applicable thresholds, whereas the GDPR and the PDPL have no such thresholds. Pursuant to the Guideline on Data Controllers and Data Processors issued by the Turkish Personal Data Protection Authority ("the Authority"), data controllers are determined based on who decides with regard to the following matters: • collection of personal data and the collection method, • categories/types of personal data to be collected, • purposes of use of the personal data collected, • which individuals' data is to be collected, • whether the personal data collected is to be shared, if yes, with whom, • the period of storage of the personal data collected.
Issue: Disclosure/Transparency Obligations			
At or before the point of collection, a business should inform consumers as to: • the categories of personal information to be collected and, • the purposes for which the categories of personal information shall be used. A business should disclose in its privacy policy (and update at least every 12 months):	The controller, while collecting from the data subject, is under an obligation to provide at the time of collection: • the identity and the contact details of the controller; • any recipients or categories of recipients of the personal data; • the legal basis and purposes for the processing (if the controller then intends	Pursuant to PDPL and the Communiqué on the Principles and Procedures to be Followed in the Fulfilment of the Obligation to Inform; the data controller or the persons authorized by the data controller is obliged to inform the data subjects while collecting the personal data with regard to; • the identity of the data controller;	The scope of disclosures required by the GDPR extends beyond that required by the CCPA. Most of the types of information required to be disclosed by the CCPA are also required to be disclosed under the GDPR and the PDPL. However, even where the disclosure requirements are similar, there are some subtle differences. For example: • while the GDPR undoubtedly requires disclosure if personal data is

CCPA	GDPR	PDPL	Comments
• a description of consumers' specific rights under the CCPA and the methods provided by the business for consumers to submit corresponding requests (including if the business sells personal information, a link to a "Do Not Sell My Personal Information" webpage). • lists, in respect of the preceding 12 months, of: • the categories of personal information collected • and • the categories of personal information disclosed (for a business purpose) or sold (or a statement that the business has not engaged in such sale or disclosure, if applicable).	to process the personal data for a different purpose, it must inform the data subject before doing so); • the retention period for the personal data, or if not possible, the criteria used to determine that period; • the rights of access, rectification, deletion and portability of personal data, to restrict or object to processing and to complain to a supervisory authority; • where applicable, information about: the controller's representative and data protection officer; the legitimate interests for processing; exports of the personal data out of the EEA; the right to withdraw consent • whether the provision of personal data is required by law or in connection with a contract (and if the data subject is obligated to provide the personal data and the possible consequences of not doing so); • any automated decision-making, including profiling, with at least meaningful information about the logic involved, the significance and the envisaged consequences for the data subject; • the source of the personal data (where not obtained from the data subject).	• the purposes for which personal data will be processed; • the persons to whom processed personal data might be transferred and the purposes thereof; • the method and legal reason of collection of personal data; • the rights of the data subject including rights of access, rectification, deletion and destruction of personal data, compensation, object to occurrence of any result that is to data subject's detriment by means of analysis of personal data exclusively through automated systems; • where applicable, information about the controller's representative. If the processing purpose changes, the obligation to inform shall be fulfilled before the data processing activity takes place for the latter purpose.	being sold, it does not include very prescriptive obligations of the kind reflected by the CCPA; • the CCPA requires some disclosures only in respect of the previous 12 months, whereas the PDPL and the GDPR have no such limitation; and • while the PDPL GDPR and the CCPA require the disclosure of the rights available to applicable individuals, the rights themselves are also not identical. Therefore, existing privacy policies (even those tailored for the GDPR and the PDPL) will not automatically be fit-for-purpose for the CCPA and will likely need to be updated to reflect its requirements.

CCPA	GDPR	PDPL	Comments
Issue: Right of Access (and portability)			
A consumer has the right to request the disclosure from a business of the: • specific pieces of information collected; • categories of information collected; • categories of third parties with whom the information is shared; • categories of sources of the information; • business or commercial purpose for collecting or selling personal information. A business that receives a verifiable request relating to the above is required to make the disclosure free of charge, within 45 days; however, it is not required to provide personal information to a consumer more than twice in a 12-month period. The disclosure should be made in writing and delivered either: through the consumer's account with the covered entity, if they have one (if not they should not be asked to create one); by mail; or electronically, at the consumer's option if they do not have an account (in which case the information must be provided in a readily useable format that allows the consumer to easily transmit the information to another entity).	A data subject has the right to confirmation from the controller about whether personal data about them is being processed; and, if so: • a copy of the personal data; • the categories of personal data concerned; • the recipients or categories of recipient with whom the data may be shared (particularly outside the EEA or international organizations, with information about the corresponding safeguards); • any available information about the source (where not collected from the data subject); • purposes of processing; • the existence of the rights of access, rectification, deletion and portability of personal data, to restrict or object to processing and to complain to a supervisory authority; • the retention period for the personal data, or if not possible, the criteria used to determine that period; • any automated decision-making, including profiling, with at least meaningful information about the logic involved, the significance and the envisaged	Although under the PDPL, data subjects do not have the right to access the data itself, Art. 20 of the Constitution of the Republic of Turkey grants everyone the right to request the protection of her/his personal data, which includes the right to access to her/his personal data, to be informed about her/his personal data, request their rectification or erasure and know whether they are used in accordance with the purposes determined. Under the PDPL, the data subject has the right to be informed whether her/his personal data has been processed, and to request information as to processing, if her/his data have been processed. When a data subject makes a request to the data controller in accordance with the PDPL, the data controller is obliged to respond as soon as possible depending on the nature of the request and at the latest, within 30 days. As a rule, the response shall be free of charge; however, if it requires an additional cost, the data controller may charge the data subject the fee determined by the Turkish Personal Data Protection Board. The data controller's response shall be delivered in an electronic or written form.	The access right gives applicable individuals rights to obtain much of the same information that the business is also required to disclose in any event. The right of access are somewhat similar in some respects between the CCPA and the GDPR. In addition: • the GDPR also gives data subjects the right to information about their other rights, although the CCPA does require the information about similar rights to be disclosed to consumers; and • the GDPR is broader in scope than the CCPA, giving rights to information about the retention period and any automated decision-making. Beyond the right of access, the GDPR offers an additional "right to data portability" in certain circumstances. The right to data portability allows the data subjects to obtain and reuse their personal data for their own purposes across different services. Data portability allows data subjects to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way without affecting usability. The CCPA goes part way towards a similar right, by providing that the a business responding to a consumer's access request must (at the consumer's option) provide the information electronically in a readily useable format that allows the consumer to easily transmit the information to another entity. However, unlike the GDPR, the CCPA does not go as far as to

CCPA	GDPR	PDPL	Comments
	consequences for the data subject. The controller generally is obligated to comply with a request free of charge without undue delay and in any event within one month of receipt. Where the request was made by electronic means, and unless otherwise requested by the data subject, the information should be provided in a commonly used electronic form. In certain circumstances, a data subject has additional rights to: • receive a copy of their personal data in a structured, commonly used, machine-readable format; and • transmit the data to another controller without hindrance from the original controller, including to have the personal data transmitted directly from the first controller to the second controller.		give a consumer a right to require the business itself to transfer the information to another business. The PDPL does not give any right to data portability. Businesses that have implemented processes for responding to data subjects' requests for access and portability under the GDPR may, in theory, be able to apply those processes in relation to the CCPA. However, not updating and tailoring those processes to the CCPA might miss nuanced differences in the relevant requirements and, in any event would involve the business "over-complying," in particular by giving consumers a much wider scope of information than is required by the CCPA and by offering consumers rights (to portability to another business) that are not available under/required by the CCPA.
Issue: Right to Deletion/Erasure ("right to be forgotten")			
A consumer has the right to request deletion of personal information a business has collected from them. A business that receives a verifiable request relating to the above is obligated to delete the consumer's personal information from its records and direct any service providers to delete	A data subject has the right to erasure by the controller of personal data about them in certain circumstances, namely if: • the data is no longer needed for its original purpose (and no new lawful purpose exists);	Pursuant to PDPL and the Regulation on Erasure, Destruction and Anonymization of Personal Data, upon disappearance of the legal grounds provided in the Articles 5[1] and 6 of the PDPL on which the processing is based, the data controller is obligated to erase, destruct or anonymize the personal data, ex officio	There are several differences between the deletion right (and corresponding obligations on businesses) under the CCPA and the PDPL: The CCPA's deletion right applies only to data collected from the consumer (i.e. not to data about the consumer collected from third party sources), whereas the PDPL's applies to all data concerning a data subject.

[1] Art. 5/2 of PDPL: "Personal data may be processed without seeking the explicit consent of the data subject only in cases where one of the following conditions is met: **(a)** it is clearly provided for by the laws; **(b)** it is mandatory for the protection of life or physical integrity of the person or of any other person who is bodily incapable of giving his consent or whose consent is not deemed legally valid; **(c)** processing of personal data belonging to the parties of a contract, is necessary provided that it is directly related to the conclusion or fulfilment of that contract; **(ç)** it is mandatory for the controller to be able to perform his legal obligations; **(d)** the data concerned is made available to the public by the data subject himself; **(e)** data processing is mandatory for the establishment, exercise or protection of any right; **(f)** it is mandatory for the legitimate interests of the controller, provided that this processing shall not violate the fundamental rights and freedoms of the data subject."

CCPA	GDPR	PDPL	Comments
the consumer's personal information from their records. "Service provider" means a for-profit legal entity that processes information on behalf of a business and to which the business discloses a consumer's personal information for a business purpose pursuant to a written contract (containing certain prohibitions). Neither a business nor a service provider is required to comply with a consumer's deletion request if the personal information is necessary for the business or service provider to: • complete a transaction for which the personal information was collected, provide a good or service requested by the consumer or otherwise perform a contract between the business and the consumer; • detect security incidents; • protect against malicious, deceptive, fraudulent or illegal activity (or prosecute those responsible); • debug to identify and repair functionality errors; • exercise or ensure the right of another to exercise free speech or another legal right; • comply with the California Electronic Communications Privacy Act, which compels the production of or access to electronic	• the processing is based on consent, and the data subject withdraws consent (and no other lawful ground exists); • the data subject exercises the right to object, and the controller has no overriding grounds for continuing the processing; • the data has been processed unlawfully; or • erasure is necessary to comply with EU or EU Member State law. The controller is obligated to delete the data without undue delay and in any event within one month of receipt of the request. The controller is also obligated notify to each recipient to whom the personal data has been disclosed (unless this proves impossible or involves disproportionate effort). Where the controller has made the personal data public, the controller is obligated to take reasonable steps to inform other controllers processing the personal data that the data subject has requested deletion of any links to, or copy or replication of, that personal data. The deletion obligations do not apply where the processing: • is necessary for exercising the right of freedom of expression and information; • for compliance with EU or EU Member State law;	or upon demand by the data subject. However, the data subject does not have the right to request anonymization of her/his personal data in any event. When a data subject requests the erasure or destruction by the controller of personal data about them; • if all the legal grounds to process has disappeared, the data controller erases, destruct or anonymizes the relevant personal data in thirty days at the latest and informs the data subject thereof. • if all the legal grounds to process has disappeared and the personal data was transferred to third parties, the data controller informs the relevant third parties and ensures the third party to fulfill its obligations with respect to erasure, destruction or anonymization. • if all the legal grounds to process have not entirely disappeared; the data controller can deny the request of the data subject with an explanation for denial, and it informs the data subject thereof in writing or by electronic means in thirty days at the latest. The data controller is obliged erase, destruct and anonymized the personal data in accordance with its policy on storage and destruction of personal data and technical and administrative measures.	While the CCPA and the PDPL have exceptions, in relation to which the applicable deletion right does not apply (see below), the PDPL also limits the circumstances in which the underlying right to deletion applies. However, these circumstances are broad enough to apply to most exercises of the right by data subjects. The exceptions to the CCPA's deletion right are much broader than exceptions under the PDPL, and include circumstances such as where the information is needed: for a contract, free speech and internal uses aligned with the consumer's expectations / the context in which the consumer provided the information. These are broad enough to potentially eliminate a consumer's deletion rights under the CCPA in most, if not all, circumstances. A business that has implemented measures pursuant to the GDPR's right to deletion (both to minimize and comply with requests) is unlikely to be able, or want, to simply apply the same measures to requests under the CCPA, and doing so would grant much broader deletion rights to consumers than are provided for by the CCPA. Instead, a close examination of the uses of personal information by the business and the corresponding circumstances in which the business will be obligated to comply with deletion requests should help the business both minimize and comply with requests under the CCPA. Even though right to be forgotten is not defined under the PDPL, with the recent jurisprudence of the Turkish Constitutional Court and the Assembly of Civil Chambers of the Court of Appeal, the right to be forgotten has been accepted.

CCPA	GDPR	PDPL	Comments
communication information or electronic device information with a search warrant; • engage in research in the public interest (if the consumer has provided informed consent); • to enable solely internal uses aligned with the consumer's expectations given their relationship with the business; • comply with a legal obligation; • otherwise use the information internally in a lawful manner compatible with the context in which the consumer provided it.	• for a task in the public interest or in the exercise of an official authority of the controller; • in the public interest in public health; • for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, • for the establishment, exercise or defense of legal claims.	The data controller is obliged to erase, destruct or anonymize personal data in the first periodic destruction following the date upon which the obligation to erase, destruct or anonymize personal data occurs. The period of time, during which periodic destruction is carried out, shall be determined and observed by the data controller in its personal data storage and destruction policy. This period cannot exceed six months at any time. In the case that the data controller does not have the obligation to prepare a personal data storage and destruction policy, it is obligated to erase, destruct or anonymize personal data within three months from the date upon which the obligation to erase, destruct or anonymize personal data occurs. The data controller shall keep erasure, destruction or anonymization of personal data records for at least three years.	
Issue: Right to Opt-Out			
A consumer has the right to require a business, that sells (broadly defines as "selling, renting, releasing, disclosing, disseminating, making available, transferring or otherwise communicating orally, in writing, or by electronic means, a consumer's personal information by the business to another business or a third party for monetary or **other valuable consideration**) personal information to third parties, not to sell the	There is no express right for data subjects to opt out of the sale of their personal data under the GDPR; however, under the GDPR while processing personal data, any controller (including a business engaged in the sale of personal data) is subject to obligations in order to provide and inform data subjects about a lawful basis for processing, and also, for example, to inform data subjects about the purposes of the processing and inform	There is no express right for a data subjects to opt out of sale of their personal data under the PDPL; however, under the PDPL while processing personal data, any controller (including a business engaged in the sale of personal data) is subject to obligations in order to provide and inform data subjects about a lawful basis for processing, and also, for example, to inform data subjects about the purposes of the processing and inform	While the CCPA includes a specific right to opt out of the sale of personal information which the GDPR and PDPL do not, the GDPR and the PDPL include much broader rights for data subjects to restrict and object to the processing of their personal data more generally. Therefore, despite the absence of an express right to opt out (of data sale), the GDPR nevertheless presents significant challenges to any business that sells personal data (particularly as its business model).

CCPA	GDPR	PDPL	Comments
consumer's personal information (opt out). A business is prohibited from selling personal information of a consumer: • from whom it receives a request to opt out (unless and until it has subsequently received the consumer's express authorization to do so, which it cannot request for at least 12 months after receiving the opt -	data subjects of their rights, in particular their rights to withdraw consent (if consent is the lawful basis) and/or object to such processing.	data subjects of their rights, in particular their rights to withdraw consent (if consent is the lawful basis) and/or object to such processing.	A business that sells personal data and has implemented measures pursuant to the GDPR is unlikely to find that those measures align with the requirements of the CCPA and is likely to need to implement separate measures in light of the CCPA (or to choose the "highest common denominator" approach). The PDPL does not have any provision for selling the personal data. However Turkish Criminal Code numbered 5237 strictly prohibits the unlawful delivery and recording of personal data. The Law on the Regulation of Electronic Commerce numbered 6563 refers specific fines for unsolicited messages. In a recent decision, the Turkish Personal Data Protection Board (2018/119) resolved the seizure of the data processing activities of a data controllers processing personal data without the explicit consent of the data subject.
out request). • who is a minor if it has not received consent (i.e., opt in): • whom the business has actual knowledge is under the age of 16, unless: • the consumer is between 13 and 16 and has opted in; or • the consumer is less than 13 years of age and the consumer's parent or guardian has opted in on the consumer's behalf.			
Issue: Processors			

CCPA	GDPR	PDPL	Comments
The right to deletion under CCPA includes an obligation on a business to direct any service providers, which are entities that the business has disclosed personal information for processing on behalf of the business, to comply with the deletion request; the CCPA implicitly requires the service provider to comply with such request; however, the CCPA does not otherwise include detailed obligations on or in relation to "processors". Service providers, as well as businesses are liable for civil penalties under the CCPA but service providers are not liable for failure by a business that shares data with them to comply with its CCPA obligations.	The GDPR imposes detailed obligations on controllers in relation to processors, and directly on processors.	The PDPL does not impose specific obligations on data processors, however, data controllers and processors are jointly liable for providing data security, and taking administrative and technical measures thereof.[2]	Businesses that engage processors that are "service providers" under the CCPA may want to seek to impose contractual obligations on such service providers to comply with deletion requests, e.g., in data processing agreements (that may have been implemented / updated pursuant to the GDPR.) Entities that act as service providers under the CCPA may consider both: • anticipating notification from their CCPA business-customers of consumers' deletion requests and implementing procedures to comply; and • seeking to impose requirements on their CCPA business-customers to provide notification as required (e.g., in relevant data processing agreements, as above. Much like the GDPR, the CCPA may provoke detailed negotiations and "battles of the forms" as customers and vendors seek to impose contractual obligations on each other in relation to requirements of the CCPA—not only to comply with its requirements but also to control how the entity complies. Under the PDPL, the data processors are obliged to take following measures with the data controller; • prevent unlawful processing of personal data; • prevent unlawful access to personal data; • safeguard personal data.

[2] For more detailed explanation see 'Right to Deletion/Erasure'.

GKC Partners

Ferko Signature

Büyükdere Cad. No: 175 Kat: 10

Levent 34394 Turkey

T + 90 212 355 1300