dataprotectionlaw&policy

STRATEGIC ANALYSIS BY DATAGUIDANCE
FEBRUARY 2015 VOLUME 12 ISSUE 02
WWW.E-COMLAW.COM

APEC agrees processor certification

The Asia Pacific Economic Cooperation (APEC) Data Privacy Subgroup ('DPS') agreed, on 3 February 2015, on a new cross border certification system for data processors entitled 'APEC Privacy Recognition for Processors' ('the PRP').

"The PRP will allow processors to formally demonstrate their ability to effectively implement a controller's privacy obligations under the APEC Cross Border Privacy Rules (CBPR) system," said Markus Heyder, Vice President at the Centre for Information Policy Leadership at Hunton & Williams LLP. "In turn, controllers will also be able to identify qualified and accountable processors as a result of the PRP. With the PRP in place, the CBPR system will now cover both controllers and processors, and thus the entire information-handling ecosystem."

The PRP will consist of 17 requirements that a processor must implement. Accountability Agents will review and certify compliance with the PRP. Before the PRP can be launched, it has to be integrated into the CBPR governance structure.

IN THIS ISSUE

Dutch data retention bill neglects CJEU judgment

The Dutch Data Protection Authority (DPA) issued, on 16 February 2015, a letter to the Ministry of Security and Justice advising on a draft bill ('the Bill') which would amend the Telecommunications Data Retention Act and the Criminal Code, and regulate the retention of data processed in connection with public electronic communications.

The DPA found that the Bill was inconsistent with the necessity and proportionality principles, and suggested that it should not be submitted to Parliament as it would require the 'retention of historical telephony and internet data of virtually all Dutch citizens for six to twelve months,' and to introduce a prior review procedure run by the judiciary on accessing historical telecommunications data, among others.

Introduced in 2014, the Bill follows the Court of Justice of the European Union (CJEU) ruling, which found the EU Data Retention Directive (2006/24/EC) ('the Directive') invalid in Joined Cases C-293/12 (Digital Rights Ireland) and C-593/12 (Seitlinger) in April 2014.

Gerrit-Jan Zwenne, Partner at Bird & Bird LLP, said, "The Bill only addresses one or two of the problems identified by the CJEU in its decision, i.e., the security requirements and for data not to be transferred outside of the EU. All the other issues are neglected in the Bill."

Separately, on 18 February 2015, a hearing was held before the District Court of The Hague in the injunction proceedings against the Dutch Government, initiated by a group of organisations and which aim to invalidate the Dutch Telecommunications Data Retention Act ('the Act') in force, on the grounds of it breaching the fundamental right to privacy. A ruling is expected on 11 March 2015.

Fulco Blokhuis and Otto Volgenant, Partners at Boekx Advocaats, the law firm representing the plaintiffs, said, "The Act still fully mirrors Directive 2006/24/EC, even if the Dutch Government has indicated that it is willing to amend the current Dutch data retention obligation. While a bill has been drafted, no draft act has been presented to Parliament yet."

Volgenant added, "It is unacceptable that the Government holds on to this practice after the CJEU has already clearly ruled that this is a privacy violation. Dutch telcos and internet service providers (ISPs) still have to retain and disclose communications data at the request of the Government."

WP29 clarifies scope of further health data processing in apps

The Article 29 Working Party (WP29) issued, on 5 February 2015, a letter to the EU Commission ('the Commission') addressing a request to clarify the scope of health data in the context of wellbeing and lifestyle apps.

In particular, the WP29 stated that under the current Data Protection Directive (95/46/EC) further processing of mHealth personal data (even pseudonymised) for historical, statistical and scientific research purposes should only be permitted under explicit consent, with exceptions laid down in national law. 'Any proposals to weaken and thereby broaden the scope of this type of processing […] should be negatively assessed,' read the letter.

"The WP29 is clearly distancing itself from the Draft General Data Protection Regulation (GDPR) in relation to the further processing of health data for historical, statistical and scientific purposes is concerned and is in line with the other opinions of WP29," said Monica Oliveira Costa, Partner at Coelho Ribeiro e Associados. "However, this does not necessarily mean a step back on the data protection reform."

William Long, Partner at Sidley Austin LLP, added, "With a few months to go [on the adoption of the GDPR], it is clear that the need to strike the right balance, whether it be in relation to specific aspects, such as pseudonymised data or the whole Regulation, is critical."

A new age of personal data protection dawns in Turkey

A draft Turkish bill, inspired by the European Data Protection Directive 95/46/EC, contains the building blocks for a privacy regime which would introduce such concepts as prior notification of data subjects, registration with the data protection regulator and restrictions on data transfers. In this article, Begüm Yavuzdoğan Okumuş, Bentley James Yaffe and Alp Turan, Senior Associate, Associate and Trainee respectively at Gün + Partners in Istanbul, discuss the relevant provisions of this bill and its potential impact on companies that are doing business in the country.

With internet usage becoming increasingly widespread and the new boost in global technologies for commercial and personal use, the volume of personal data that is collected, processed and transferred has also increased. In Turkey, where previous attempts at passing a specific data protection law have failed, many areas of uncertainty exist in relation to the individual rights of data subjects and the responsibilities of companies and entities that collect and process data. In the absence of a specific law, the Turkish Constitution governs privacy matters in a very general way.

However, on 26 December 2014, the Turkish Prime Minister's Office finally sent the long awaited Draft Law on the Protection of Personal Data ('the Draft Law') to the Directorate of the Turkish Parliament. It is widely expected that the Draft Law will come into force soon.

The Draft Law was prepared in parallel with EU Data Protection Directive 95/46/EC rather than the more recent Directive Proposal 2012/0010/COD. It is suggested that the Draft Law should be revised to take account of the latest developments in Europe. Various non-governmental organisations and associations have made suggestions for amendments and there may be changes to the Draft Law in line with the proposals received from certain industry players.

Companies based in Turkey or which have business relations with Turkey must be prepared for the enactment of the Draft Law since it will feature innovative concepts, rules and regulations, as well as the establishment of a regulatory authority, the Data Protection Authority (DPA).

The draft law

Personal data is currently protected under the Constitution and the general provisions of the Code of Obligations and the Criminal Code. So far, data protection regulations have only been implemented through a limited sector-based approach, such as those concerning electronic communications and healthcare. However, many essential elements, such as procedures relating to the transfer of personal data to third countries or how explicit consent is to be recorded by data processors, are not clear. Consequently, industry players have repeatedly stated the need for general data protection legislation.

If passed by Parliament, the Draft Law would, for the first time, introduce an overarching data protection regime establishing the general rules for the processing, storage and transfer of data of data subjects in Turkey. The Draft Law would apply to any natural or legal person who processes personal data, whether such data is processed in full or in part, automatically or manually.

Impact on companies processing data in Turkey

Explicit consent

The primary principle states that personal data cannot be processed without the explicit consent of the data subject. Under the provisions of the Draft Law, personal data can only be processed if (i) the processing is in accordance with the law and the principle of good faith; (ii) the data is accurate and kept up to date; (iii) the data is processed for specified, clear and legitimate purposes; (iv) the processed data is used in accordance with and for the purpose of processing and the processing is proportionate with such a purpose; and (v) the data is stored only for the length of time required for the purpose of processing.

The Draft Law includes exceptions where explicit consent would not be required. For example, data processors need not obtain consent where the processing is clearly foreseen by law, or where it is necessary for the establishment or performance of a contract that the data subject is party to, or where the data has been made public by the data subject.

Sensitive data

The Draft Law also defines special categories of personal data which cannot be processed at all, apart from the exceptions specifically enumerated for these categories. These special categories concern data relating to race, ethnic origin, political opinion, philosophical belief, religion, denomination or other beliefs, memberships of associations, charities or unions and health or sexual life of individuals.

Data controllers have three main obligations under the Draft Law: (i) the duty to notify; (ii) the duty to ensure that personal data is

stored and processed securely; and (iii) the duty to register with the Register of Data Controllers.

Duty to inform data subjects

The data controller must inform the data subjects about the identity of the company, the purposes for processing, and whether such data can be transferred to third parties and if so, for what purpose, together with how their data is being collected and the grounds for such processing. It also states that data controllers must notify subjects if personal data is erased, destroyed or anonymised.

Duty to notify

The duty to notify requires that the subject be informed as to the identity of the data controller, the purpose and/or grounds for processing, to whom the personal data may be transferred, and all other rights that the subject has under the Draft Law.

The duty of secure storage and processing requires the data controller to establish the necessary safeguards for the sufficient protection of data. If the data controller determines that third parties have illegally accessed personal data, it must notify the DPA as soon as possible.

Data transfers

As regards data transfers, the primary principle under the Draft Law establishes that personal data cannot be transferred to foreign countries unless the subject has provided explicit consent. However, if one of the exceptions to the principle of explicit consent is present, personal data may be transferred to third parties, provided that sufficient safeguards exist within the foreign countries. If the foreign country in question does not possess sufficient safeguards, the transfer may only take place if the data subject provides explicit consent or if the data controllers in the foreign country give a written undertaking to provide sufficient safeguards and the DPA permits such transfers. The transfer of special categories of data is subject to even stricter conditions in that, along with the consent of the data subject and the existence of sufficient safeguards in the recipient country, permission of the DPA is required.

Companies based in Turkey or which have business relations with Turkey must be prepared for the enactment of the Draft Law since it will feature innovative concepts, rules and regulations, as well as the establishment of a regulatory authority, the Data Protection Authority

Data security obligations

The data controller shall be jointly and severally liable with the person who is processing the personal data on behalf of itself, and shall take the necessary precautions to ensure that data is processed securely in line with the law.

How can companies prepare themselves for the new regime?

It is worth mentioning that data controllers which fail to comply with their obligations will be subject to heavy administrative fines under the Draft Law, ranging from TRY 1,000 to TRY 100, 000 for failure to notify, and from TRY 10,000 to TRY 1,000,000 for failure to comply with their duties of registration and secure processing and storage. In the light of these sanctions, it is essential for companies that process personal data to ensure that mechanisms are established to provide the required notification to data subjects, and to ensure that data is securely stored and processed.

As the definition of explicit consent is not specified within the Draft Law, companies should ensure that it is received in writing - either through an actual or electronic signature - and the data subject is sufficiently informed as to the exact scope of the processing.

Companies that process personal data should also ensure that they have a designated contact address in order to appropriately receive and log any complaints made by data subjects. Additionally, internal processes should be established in order to address any complaints and make the required corrections.

All personal data that has already been processed must be aligned with the Draft Law within two years of its implementation. Consequently, all real and legal persons who have previously processed personal data must ensure that personal data is stored, processed and transferred in accordance with the Draft Law.

Although the Draft Law is certainly a welcomed development, there is still work to be done if Turkey is to have a modern data protection regime on par with its European counterparts.

Begüm Yavuzdoğan Okumuş Senior Associate
Bentley James Yaffe Associate
Alp Turan Trainee
Gün + Partners, Istanbul
begum.yavuzdogan@gun.av.tr
james.yaffe@gun.av.tr
alp.turan@gun.av.tr