International Law Office

EMPLOYMENT & IMMIGRATION - TURKEY

Processing employee data in light of recent DPA and court decisions

14 April 2021 | Contributed by Gün + Partners

AUTHORS

Begüm Yavuzdoğan Okumuş

Beril Yayla Sapan

The Constitution protects private life and in 2016 the Data Protection Law was enacted, furthering the protection of personal data. In disputes relating to the monitoring of employees' personal data in the workplace, the courts and the Data Protection Authority (DPA) have mostly based their decisions on the constitutional provisions. This article outlines the legal grounds for data processing in the employment context and highlights recent court and DPA decisions in this respect.

Legal grounds for data processing in employment context

The Data Protection Law provides no specific rules in the employment context. There are several circumstances in which employee data can be processed, whether it be:

- on the basis of the employee's consent;
- for recruitment purposes;
- for the performance of contracts;
- for employers to fulfil obligations set out by law;
- for the management and planning of work;
- to ensure health and safety at work;
- for the purposes of exercising and using rights and benefits relating to employment; or
- for the purpose of terminating employment relationships.

Unlike the EU General Data Protection Regulation (GDPR) (Article 9/2/b), sensitive data is processed under limited conditions in Turkey, especially in terms of processing data relating to health or sexual orientation, where processing is possible only based on obtaining explicit consent and in limited cases. Sensitive data other than that relating to health and sexual orientation can be processed only when it is required by law. Thus, employers must follow the consent mechanism under Turkish data protection law. Consent must be freely given and prior to giving consent, the data subject must be informed. It must be distinguishable from other matters. Further, it is the data controllers' liability to demonstrate that the data subject has been informed and given its consent.

Data controllers' key obligation is to inform data subjects

Under the Data Protection Law, like under the GDPR, controllers must inform data subjects about data processing activities.

Therefore, to ensure compliance with data privacy laws in the workplace, employers must ensure that they have certain provisions in employment agreements. In any case, a privacy notice must be prepared separately and employees must be informed of data processing procedures in detail with a separate document.

Processing biometric data and monitoring

The most debated issues in Turkey with respect to privacy in the employment context relate to the processing of biometric data and employee monitoring, which may include in-vehicle monitoring and systematic or on-the-spot monitoring of corporate emails.

Processing biometric data

In terms of processing biometric data, the DPA issued a decision relating to a gym. The DPA found that processing gym members' biometric data when they entered the building was not lawful even if the gym had members' explicit consent and also provided them with an alternative option to enter the gym using a pass card. The DPA concluded that processing biometric data is not proportionate with the purpose of the processing and in cases where there are other less intrusive tools that could achieve the purpose there is no necessity to process biometric data. This decision will affect workplaces where companies use, for example, retinal scan technologies for building entrances. However, the DPA's decision must not be interpreted as if processing biometric data is prohibited for all workplaces; it can still be processed by obtaining data subjects' explicit consent where there is a necessity or to ensure a high level of security.

In-vehicle monitoring

In-vehicle monitoring also applies in workplaces. When a vehicle is linked to a specific employee, personal data will be processed through in-vehicle monitoring systems. There must be a necessity for the specific position of the employee where the employer is required to monitor their location during working hours to audit the activities or time spent out of the office. However, such an application must be proportionate with the purpose of the processing. Further, if private use of the vehicle is also allowed, employees' consent must be obtained or in-vehicle monitoring hours must be restricted if possible. Employees must be informed of in-vehicle monitoring systems beforehand. Proportionality is the key element to evaluate in this regard. As the data controller will likely rely on the legitimate interest legal ground, while implementing monitoring, the balance between employers' interests and employees' rights and freedom must be diligently evaluated.

Monitoring corporate emails

Monitoring corporate emails (whether it be systematic or on the spot) has many risks from a privacy law perspective. The DPA and the courts have ruled in several decisions in this respect.

Employers collect corporate records and back up emails to ensure the security of the system or to be able to investigate any allegation of corruption. In principle, monitoring is not prevented by laws; however, it must be justified, necessary and proportionate.

In a January 2020 decision, the DPA concluded that the data controller (employer) that had monitored employee emails had processed personal data to exercise its legal rights. Therefore, the DPA held that the processing had been made lawfully.

Courts' approach towards employee data processing

Before the enactment of the Data Protection Law, the Supreme Court had already accepted that employers can monitor employees' email correspondences as long as the employer's computer and equipment are used.

In April 2016, just before the enactment of the Data Protection Act, the Constitutional Court ruled in a decision concerning the monitoring of employees' corporate emails. In this decision, it was said that the employees had been informed through their internal regulations that their corporate email accounts could not be used for private use and that the employer had the right to monitor correspondence.

The Constitutional Court found no violation of the right to privacy and privacy of communication as the employer had already made notifications and warnings to the employees regarding the monitoring of their email correspondence. Thus, even before the enactment of the Data Protection Law, the Constitutional Court highlighted the importance of the informing obligation.

In May 2019, in line with the Data Protection Law and the Constitutional Court's decision, the Supreme Court held that within the scope of employers' right to manage, employers can monitor employees' electronic communication. However, to do so, the employees must be reasonable informed by their employer about the monitoring of correspondence.

Recently, the Constitutional Court also ruled in two decisions concerning the monitoring of employees' corporate emails. In October 2020 the court ruled in an application filed by an employee of a law firm, concluding that the employer had not duly informed the employee about its monitoring activities and that the employer had breached the principle of proportionality by examining correspondence with third parties, as the inspection that took place had not been limited to the allegations in question (for further details please see "Constitutional Court rules on employers' review of employees' corporate emails").

In January 2021 the Constitutional Court ruled in another decision and found no violation of the rights of personal data protection and the freedom of communication (for further details please see "New Constitutional Court ruling on employers' inspection of employees' corporate emails"). The Constitutional Court further stated that the employee's employment contract stipulated that:

- the employee corporate email was for only business use; and
- the bank management could carry out an inspection at any time without prior notification.

Therefore, the Constitutional Court ruled that the employer had fulfilled the explicit information requirement and the employee had consented to the inspection by signing the employment contract. The Constitutional Court ruled that the employer had conducted an inspection limited to the purpose of processing and used the collected data in compliance with the purpose.

Comment

The DPA and the courts have similar approaches in evaluating employee data processing disputes. They all hold that fundamental to data processing are the principles of:

- necessity;
- purpose specification;
- transparency;
- legitimacy; and
- proportionality (when processing employee data in the workplace).

Informing employees beforehand about data processing activities is key and may affect parties' litigation strategies in the future.

For further information on this topic please contact Begüm Yavuzdoğan Okumuş or Beril Yayla Sapan at Gün & Partners by telephone (+90 212 354 00 00) or email (begum.yavuzdogan@gun.av.tr or beril.yayla@gun.av.tr). The Gün & Partners website can be accessed at www.gun.av.tr.