

May 24, 2019

Almost one year after the GDPR became applicable; Hungary enacted the long-awaited Data Protection 'Salad' Act. The Data Protection 'Salad' Act modified 86 Hungarian acts pursuant to the deregulation and implementation of the GDPR with the aim of bringing the Hungarian regulatory framework in line with the GDPR. The most important changes are the following:

Retention period for camera records (CCTV)

The previous rules governing the retention period for surveillance camera records (3 days, 30 days and 60 days, as applicable) have been repealed. Data controllers may now decide how long they wish to keep such records for, while taking into consideration that they are still obliged to comply with the limitations relating to the storage of such retained records and the purpose of retention. In line with applicable principles, data controllers may only store records for a period deemed necessary for the purposes of camera surveillance. To justify their legitimate interests, data controllers are required to prepare legitimate interest tests (balancing tests) relating to the data processing in connection with camera surveillance. As a further change to the regulations governing camera surveillance, security surveillance may only take place in private areas. In addition, data controllers are obliged to keep records (either in electronic or in paper form) of the persons viewing the video recordings, as well as the purpose and time of such viewing.

Whistleblowing

Under the new rule, companies are now entitled to process sensitive data and personal data relating to criminal records in the reporting system.

Retention period for documents related to employment relationships (employment agreements, payroll records, working time records)

Recent amendments to social security legislation settled ambiguities connected to the obligation of employers to retain archived data relating to past employees. Act LXXXI of 1997 on Social Security Pension Benefits now makes it clear that such archived employment-related documents relevant to establishing pension benefits must be retained by employers until the expiry of a period of five years after the affected (former) employee reaches retirement age.

Private use of devices and platforms provided to employees by their employer

Act I of 2012 on the Labor Code (the “Labor Code”) now prescribes that devices and platforms provided to employees by their employer may be used only for fulfilling work duties unless the parties explicitly allow private use of such devices and platforms in the employment agreement or a policy issued by the employer. The previous legislation allowed private use in general, unless such use was prohibited by the employment agreement or a pertinent policy.

Bring your own device

Devices and platforms used for work duties may be searched and reviewed by the employer regardless of whether such devices and platforms belong to the employer or the employee. Employees must be informed of the possibility of such searches during onboarding and ideally be frequently reminded thereof afterwards. Verifying compliance with the prohibition of private use is an acceptable ground for undertaking such searches.

Criminal background checks

Employers may only process criminal record data in respect of employees/candidates who are applying for positions, which (i) require the handling of firearms or poisonous, hazardous or nuclear materials, or (ii) provide access to trade secrets or potentially enable the employee to harm the financial interests of the employer. A recent guideline issued by the Hungarian Data Protection Authority clarifies that an employer may not make and retain copies or scans of criminal check certificates, but may prepare minutes with respect to the checking of a certificate’s authenticity.

Processing biometric data in the framework of employment

Biometric data relating to employees may only be processed for the purposes of identifying employees in order to protect data or objects in circumstances where unauthorized access to such data or objects could result in irreversible and severe or widespread harm to the health of individuals or overriding public or private interests (such as the security of assets with a value exceeding HUF 50 million).

Your Key Contacts



Tímea Bana
Counsel, Budapest
D +36 1 488 5200
timea.bana@dentons.com