Proskauer

French DPA Issues Robust Model Regulation for Biometric Access Controls in the Workplace

Privacy Law Blog on **April 24, 2019**

In late March, the French Data Protection Authority, Commission Nationale de l'Informatique et des Libertés ("**CNIL**") released a model regulation (the "**Model Regulation**") governing the use of biometric access controls in the workplace. Unlike many items of personal information, biometric data (such as a person's face or fingerprints) is unique and, if stolen or otherwise compromised, cannot be changed to avoid misuse. Under Article 9 of the GDPR, biometric data collected "*for the purpose of uniquely identifying a natural person*" is considered "*sensitive*" and warrants additional protections. The GDPR authorizes Member States to implement such additional protections. As such, the French Data Protection Act 78-17 of 6 January 1978, as amended, now provides that employers – whether public or private – wishing to use biometric access controls must comply with binding model regulations adopted by the CNIL, the first of which is the Model Regulation.

The Model Regulation, which the CNIL finalized and adopted following a public consultation, specifies robust requirements for the processing of biometric data for workplace access controls. Such access controls include the use of a biometric authentication system to allow entry into the workplace (or sensitive workplace areas) or access to certain databases, equipment or computer networks. Below are some of the key aspects of the Model Regulation:

- **Justify the use of biometrics**: The Model Regulation requires employers to justify the use of biometrics based upon the specific context of the workplace (e.g., the presence of dangerous machinery, valuables, confidential materials, or products subject to strict regulation) and demonstrate why the use of other traditional authentication devices (e.g., badges or passwords) is not adequate from a security standpoint. Such justification must be expressly documented by the employer, including the rationale for selecting one biometric feature over another for authentication. The Model Regulation also outlines the various types of biometric access control systems – based on the method of data transmission and storage –

and the accompanying data security risks of holding the biometric templates in a central database. It states that only critical environments would warrant stronger protections involving central databases holding biometric template data. Otherwise, the biometric data must be stored on a medium which would remain under the individual's exclusive possession (e.g., badges or smart cards) without any durable copies retained by the employer or its service providers.

- **Maintain strong data security**: The Model Regulation details many ways in which employers must maintain robust organizational and technological data security procedures. The enumerated security measures relate to the data, organization, hardware, software and computer channels, and the employer must audit, at least annually, the implementation of these measures. The Model Regulation also stipulates maximum retention periods for biometric data. For example, raw biometric data (such as a photo or audio recording) cannot be retained any longer than necessary to create a biometric template that can be analyzed by the system's software. Moreover, any resulting biometric templates must be encrypted and eventually deleted once an employee no longer works at the organization. The Model Regulation also outlines the types of individual personal data that may reside on a biometric control device and the types of log data that may be collected.
- **Remember GDPR obligations**: Beyond the Model Regulation, employers must still comply with applicable provisions of the GDPR with regard to any biometric access control system. Such compliance might include data breach notification obligations, recordkeeping requirements and compliance with the individual's data protection rights. Specifically, the CNIL noted that the collection of biometric data for access control is likely to create a high risk for the rights and freedoms of the individuals. In light of that, a data protection impact assessment must be carried out by the employer/data controller prior to the implementation of any biometric access control and updated at least every three years.

The above summarizes some of the principal aspects of the Model Regulation at a high level and, as such, the language of the Model Regulation and the CNIL's FAQ providing for additional practical commentary beyond the text of the Model Regulation should be read closely for specific requirements before instituting biometric access controls within the scope of the Model Regulation.

We note that the protection of biometric data also garners attention in the U.S., where several states have enacted biometric privacy statutes, most notably Illinois, whose statute contains a private right of action and has produced a wave of biometric privacy suits, including those against employers for using biometric timekeeping devices without adequate notice and consent. Back in the EU, the Model Regulation for biometric access controls in the workplace may conceivably serve as a model for other Member States to follow, and we will continue to follow such potential developments and further actions by the CNIL.

View Original

Related Professionals

- **Laura E. Goldsmith**
  Partner