EMPLOYEE CONSENT

Do I have to obtain employees' consent in order to collect their personal data?

The processing of any personal data may impose obligations to the individuals the data is related to, the data subjects. Some jurisdictions only recognize processing personal data as lawful if the data subject has provided express consent. Other jurisdictions require a legal obligation to process the data and may not require consent. The processing of HR personal data has raised questions and court decisions in a few countries, and interpretations may vary based on data privacy and labor law requirements.

Under Israel's Protection of Privacy Law, 1981 (PPL) "knowledgeable consent" is generally the only legal basis for processing personal data. When requesting consent from an employee, or other individual, to process their personal data, they should be given sufficient information regarding the specific matter so that they are able to assess whether to provide consent. While the PPL recognizes implicit and explicit consent, employers are expected to obtain explicit consent when processing personal employee data (per case law from the Israeli labor courts).

Employees, and other individuals, should receive a Privacy Notice if their personal data will be collected and used/retained in a computerized database. There is no specific required format, but in the context of employment, employers customarily include it in the employment agreement, in employee handbooks or in dedicated privacy policies. The notice should include (PPL, Sec. 11):

- if the individual is under a legal obligation to provide that data or, if there is no legal obligation and providing the data depends on the individual's decision and consent;
- the purpose for which the data is requested, who will be receiving the data and the purpose the data will be used for (the Privacy Notice"; and,
- in cases where data is being transferred outside of Israel, information regarding whether the individual's personal data will be transferred to third parties located outside Israel (especially in cases where a third party is located outside the European Union or the United Kingdom).

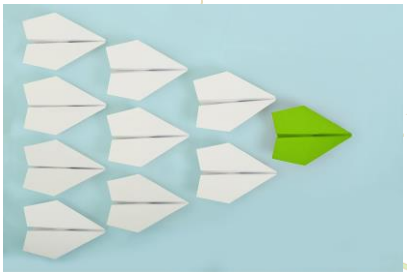
Employee Data as Sensitive Data

While the PPL includes a definition for data and sensitive data that is protected under the PPL, these terms are interpreted broadly by the Israeli courts and the Protection of Privacy Authority (PPA). The definition of sensitive data under the PPL is "information about an individual's personality, intimate affairs, health condition, financial condition, opinions and beliefs." That said, given the broad interpretation by the courts and the PPA, employee personal data is considered sensitive data. Therefore,

when processing personal employee or job applicant data, it is a best practice to only process personal data that is required to achieve legitimate purposes in the employment context. In addition, there are specific guidelines under the PPA when collecting/using biometric data (such as fingerprint data) and surveillance footage.

Though employers are required to collect employee medical data in certain instances (such as for sick or parental leave), collecting excessive medical data can be problematic under Israeli law.

Israel's Crime Register and Rehabilitation of Offenders Law, 1981, prohibits any person from directly and/or indirectly, collecting an individual's criminal background data and records, including for the purpose of employing that individual or, for making any decision relating to that individual. Note that under binding Israeli case law (CA 8189/11 Dayan v. Mifal Hapais, issued by the Supreme Court of Israel on 2 February 2013) individuals are currently allowed to provide an affidavit or a written questionnaire regarding their criminal background, subject to certain conditions and limitations. This exception is going away once the new Criminal Data and Rehabilitation of Offenders Law, 2019 goes into effect and replaces the existing law on January 16, 2021. This new law prohibits any person from collecting criminal data, both directly and indirectly.



HR Best Practices:

Obtain explicit consent from employees and job applicants prior to processing their personal data. Commit to properly informing individuals and ensuring that they receive sufficient information to provide consent, in advance of collecting and processing personal information.

Last updated September 2020.