Employee Data Privacy – Israel

Employee Access Rights

Do individuals have the right to access their personal information?

Data protective jurisdictions tend to guarantee the right of individuals to contact an organization directly and find out whether personal data is being tracked. Access procedures and acceptable exceptions (such as business secrecy) are determined by law and may be subject to the control of data protection authorities. In the context of HR, personal data access requests can include information tracked by the company as well as data tracked by third-party solutions, such as background check vendors.

Israel's Protection of Privacy Law, 1981 (PPL) gives individuals certain rights relating to their data. Under the PPL, every individual is entitled to inspect (either directly or, through a guardian or representative authorized in writing) data about themselves that is kept in a database, with some exceptions for certain databases owned by government authorities). In addition, Directive 1-2017, issued by the Israeli Protection of Privacy Authority (PPA), requires that entities that retain digital media (video calls, chat correspondence, etc.) enable data subjects to access the retained digital media data.

Where data is not held by the employer (or other owner of the database) but by a holder (such as a 3rd party payroll processor), the employer must provide the employee (or other data subject) with the contact details of the holder, and order the holder, in writing, to provide access to the requested information.

Note that there are certain instances where the right to access personal data can be denied. For instance, exceptions exist if:

- the data may cause serious harm to the data subject's physical or mental health (in this case the data may be delivered to a physician or psychologist);
- access may cause the violation of a privilege under law; or,
- if the database is maintained by certain public authorities.

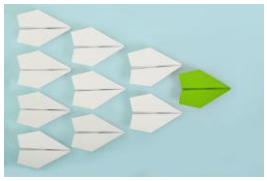
Employers (and other data owners) are required to enable employees (and other data subjects) to exercise their rights in the language of their choice (Hebrew, Arabic or English). If an individual approaches a data holder with a request to exercise their rights, the holder is responsible for informing the data subject whether they hold

information on that individual, as well as responsible for informing the individual of the name and address of the employer.

Access requests generally must be handled by the employer within 30 days, with some exceptions. If an employer refuses to enable a data subject to exercise rights under the PPL, the employer is required to notify the individual of the refusal within 21 days as of the application. The individual can choose to appeal within 30 days to a Magistrate Court.

Employees (and other individuals) who find that information on them is incorrect, incomplete, unclear or outdated can request to have their personal information amended or deleted.

Note that there are also some rights relating to data collected during the job screening process, through "Directive 2-2012 The Application of the Provisions of the Protection of Privacy Laws on Processes for Screening Applicants for Employment Purposes and the Activities of Employee Screening Centers" published by the Registrar. Under this Directive, individuals are given rights granting individuals access to screening data (including test results) maintained in a database. Note that certain data is excluded from access rights, including: details relating to the potential employer; specific characterizations of a job; and, analysis of the suitability of the job applicant and qualities and personality in relation to the job specifications.



HR Best Practices:

When processing an access request from an employee, make sure not to disclose information connected to other employees. Employers should establish official procedures and contacts for employee requests.

Last updated November 2022.