Employee Data Privacy – Israel

Security Requirements

What security obligations are imposed on data controllers and data processors?

Security requirements may not always be included in the data protection law, but are key to guaranteeing lawful processing of personal data. The entity processing the data must take all useful precautions with respect to the nature of the data and the risk presented by the processing, to preserve the security of the data and, prevent alteration, corruption or access by unauthorized third parties. Appropriate technical and organizational measures should be implemented to ensure a level of security appropriate to the risk.

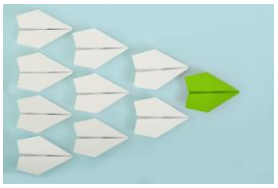
Under the Protection of Privacy Law, 1981 (PPL, Sec. 17), database owners (such as employers), databases holders and database managers are all responsible for protecting the data held in the database from exposure, use or copying without permission. Individuals who hold databases of different owners (for example, third-party payroll processors) must ensure that access to each database is given only to individuals who are authorized by written agreement between the person and the owner of the database.

The Protection of Privacy Regulations (Data Security), 2017 (DSRs) includes data security requirements based on different security levels (basic, medium and high). HR databases are generally classified as subject to the basic level (in accordance with an exclusion under the DSR) unless the database includes data relating to 100,000 or more individuals or, if there are 100 or more individuals who have access to the database. In these cases, the database is subject to the high level of security. The core obligations under the DSR include:

- formulating a database definition document;
- formulating a security procedure;
- mapping the systems and risk surveys;
- physical and environmental security;

- access permissions management;
- security event documentation;
- mobile devices;
- communication security; and,
- outsourcing.

When using outsourcing services to manage databases, agreements should be put in place and include the requirements in "Directive 2-2011 Use of Outsourcing Services for Processing of Personal Data" issued by the Registrar (the "Outsourcing Guidelines"). These Outsourcing Guidelines require that before entering into personal data processing agreements, outsourcing should be carefully reviewed to ascertain its necessity and compliance with relevant data protection laws. They should also include the: the purpose of the data transfer; the return or destruction of data upon termination of the agreement; the separate storage of data between the service provider's different clients; data subjects' access and correction rights; supervision rights on the service provider's activities; and, matters of security of the data in a binding security document.



HR Best Practices:

Ensure contracts with service providers detail the security and confidentiality measures that will be implemented. In addition, regularly train employees who may have access to personal information, to ensure that they are following all technical and organizational security measures that have been put in place.

Last updated November 2022.