The Right to Inspect Audio Data, Video Recordings, and Other Electronically Maintained Information

5/3/2017

The Israeli Law, Information and Technology Authority ("**ILITA**") recently published new guidelines outlining a data subject's right to review and inspect the personal data collected about him or her and stored in digital means.

Guideline no. 1/2017 (the "**Guideline**") will come into force on March 30, 2017.

The Right to Inspect

The Protection of Privacy Law, 1981 (the "**Law**") and the Protection of Privacy Regulations (Conditions for Inspection of Data and Procedures for Appeal from a Denial of a Request to Inspect), 1981 (the "**Regulations**"), establish the right of data subjects to review and inspect data stored in a database which relates to themselves and sets forth the procedure for such inspection.

The Purpose of the Guidelines

As a result of technological developments in the past few years, it has become common practice for entities to collect personal data via digital means such as audio, video recordings and chat correspondence. Nonetheless, the right to inspect the data, as regulated in the Law and Regulations, can be interpreted to refer, in terms of its language, only to personal data that is stored in writing and that can be provided to the data subject as a printout.

The Guidelines wish to address that issue and to clarify that the right to inspect should be interpreted broadly, in a manner that

would reflect the current practice and the technology developments. Therefore, the Guidelines clarify that the right to inspect applies also to personal data that is collected and stored in a database via digital means.

The Guidelines further clarify that the right to inspect will apply even if data is stored in a manner that is not linked to data subject's identity but such linkage is possible (even if in retrospect) with reasonable effort. "Reasonable effort" is considered to include identification based on date and time, and by using search functions available in the database. The rationale for this is that such data may be exploited, and may influence the rights of the data subject.

Implementation of the Right to Inspect - Procedure

The Regulations set forth two methods for database owners to satisfy a request from a data subject to inspect their personal data, either by presenting the personal data to the data subject, or providing the data subject with a copy of the personal data in writing. In addition, the Regulations provide that the right to inspect should be carried out in the location where the database is stored. That is, it contemplates that the data subjects will be required to physically show up in that location in order to inspect their data.

The Guidelines provide that there should be a correlation between the modern-day technology reality and the way the right to inspect is implemented. Therefore, the Guidelines clarify that the right to inspect data that is stored in digital means (such as audio and video recording) should be satisfied by allowing the data subjects to listen to the recording or to view the video containing the personal data, or by providing data subjects a copy of the digital file of the recording or video via commonly available software.

In addition, with respect to the location of the inspection, the Guidelines further state that in the current technological reality, other methods to enable inspection of data may be more efficient, quicker and generally cheaper than the current arrangement under the Regulations. Therefore the Guidelines state that it would be appropriate to deem sending files via email, granting access to a secure site or sending information via magnetic media, as meeting the intent of the Regulations.

Required Security Measures

In view of the aforesaid, the Guidelines now emphasize that upon receiving a request to inspect their personal data, the database owner must take appropriate measures to identify the data subjects, maintain the security of the data and permit access to the data solely to the data subjects or to their authorized representatives. Database owners must also prevent overbroad access to the data, which may result in violation of the privacy rights of third parties.

Sanctions

Finally, to anticipate a question our readers will ask: organizations

that breach the requirements set forth in the Guidelines are exposed to fines pursuant to the Administrative Offences Regulations (Administrative Fine – Protection of Privacy), 2004.

Contact Person

David Mirchin, Partner, Technology, IP and Data Protection

Tel: +972-3-6103199
Mail: dmirchin@meitar.com

More Information

For more information about Meitar's Technology and Intellectual Property group, click here