LEGAL UPDATE – APRIL, 2012
ILITA RELEASES DRAFT DIRECTIVE ON THE COLLECTION OF PERSONAL ID NUMBERS ("TEUDAT ZEHUT")

Recently, a hacker infiltrated a number of Israeli e-commerce sites and posted on the Internet personal information (including personal ID numbers and credit card data) relating to thousands of Israelis. Spurred by this highly publicized event, the Israeli Law, Information and Technology Authority (Israel's data protection authority, "ILITA") has issued a draft directive (the "Directive") regarding the collection of personal ID numbers ("Personal ID Numbers")[1] and passport numbers for inclusion in a database, and use of such information.

The Directive is a draft that has been circulated for public comment. If it is enacted in its current form, it will obligate certain e-commerce and other commercial entities to modify the types of information that is collected from customers and to adjust the manner in which this information is stored and used. In addition, existing databases may need to be modified to delete certain information.

General Provisions

While the Directive refers to Personal ID Numbers, it includes a note stating that its terms apply equally to passport numbers (including foreign passports).

The Directive prohibits the collection of Personal ID Numbers and their storage in a database unless the following requirements are met:

1. **Preliminary Examination and Documentation**

   Database owners must examine whether collection of Personal ID Numbers is necessary and, if so, determine for how long use of such information is required. In the context of such analysis, database owners must consider less intrusive means for data subject identification (for example, assignment of a "customer number" that is not a Personal ID Number). Results of this analysis must be documented in detail and retained by the database owner. There is no need to file the results of the analysis with the Database Registrar. The position of the Registrar is that absent a legal obligation to collect such information, collection of Personal ID Numbers will not be justified during the pre-transaction phase or in the context of a single isolated transaction (as opposed to an ongoing customer relationship), or where data subjects can be identified by other means.

2. **Disclosure and Consent**

   Personal ID Numbers may be collected only with the data subject's informed consent after receiving notice in accordance with Section 11 of the Protection of Privacy Law 1981 (the "Privacy Law").[2] The notice must be clearly worded and understandable to a reasonable person. Under the Privacy Law, consent may be express or implied; thus it can be inferred

[1] Israeli citizens are issued a personal ID number at birth. These Personal ID Numbers are used widely, and with access to an individual's personal ID number, one can learn a plethora of information about the data subject. The ID number is printed on a citizen's ID card, driver's license, passport, bank forms, army ID card, tax forms, certain business contracts to which he is a party, death certificates and wills.

[2] Section 11 of the Privacy Law requires that solicitations of database information disclose (1) whether the data subject has a legal obligation to provide the data; (2) the purpose for which data are requested; and (3) to whom data will be disclosed and for what purpose.

that a data subject who receives a compliant Section 11 notice and nevertheless provides a Personal ID Number will be deemed to have consented to the uses described in the notice even where no written consent is obtained.

3. **Purpose Limitation**

   Personal ID Numbers may only be used for the legitimate purpose for which they are collected and for the purposes to which the data subject consented, and not for any other purpose.

4. **Data Security**

   Due to the sensitivity of Personal ID Numbers, the Registrar takes the position that extra security measures must be implemented to protect such data. Encryption is recommended. If collection of the information is outsourced to a third party, Directive 2-2011 "The Use of Outsourcing for Data Processing" will apply.

5. **Data Retention**

   The database owner should evaluate whether it is necessary (pursuant to legal obligation or the nature of the transaction) to retain Personal ID Numbers following conclusion of the transaction between the parties. Where data must legitimately be retained for a longer period, such data may be used only for the specified permitted purpose, and must be stored on a segregated archive database accessible only to those requiring access. This would require database owners to maintain separate databases for current and past customers.

Scope and Implementation

If enacted, the draft Directive will apply equally to existing and new databases. If enacted, the Directive will become effective three months following the publication date, and owners of existing databases will have six months from the publication date to become compliant.

We emphasize that the current version of the Directive is a draft circulated for comment only, and if it is formally enacted, it may be modified before it is released in its final form. We will monitor this issue and report developments as they arise. ILITA is accepting comments regarding the draft Directive through May 2, 2012.

If you have additional questions concerning the subject matter of this memorandum, or would like to submit a comment to ILITA, kindly contact Yoheved Novogroder-Shoshan at Yohevedn@arnon.co.il or +972-2-623-9200.