

LEGAL UPDATE – DECEMBER, 2012

DATABASE REGISTRAR DIRECTIVE: SURVEILLANCE CAMERAS

Israel's data protection authority (the "Database Registrar") recently published Directive 4-2012 titled "Use of Security and Surveillance Cameras and Databases of Recorded Images" (the "Directive"). The Directive applies to the use of surveillance cameras in public spaces by government and non-government entities. **The Directive imposes specific requirements with respect to security and surveillance systems currently in use, as well as new systems to be implemented in the future.**

The Directive, which became effective upon publication, does not have the status of binding law. It does however indicate how the Database Registrar will interpret applicable law in the context of exercising its authority.

Companies are advised to audit current practices involving use of security and surveillance systems and related databases and institute such changes as are necessary to comply with the Directive.

Summary

The Directive was inspired by the widespread use of closed circuit television (CCTV) cameras --both live feed and recording systems--in public spaces to assist in performing security functions, as well as the use of facial recognition and LPR (license plate recognition) technology in controlling and monitoring access to buildings and parking garages.

Where use of surveillance and tracking technologies involves the processing of identified or identifiable personal information, these activities are regulated under the Protection of Privacy Law-1981 and regulations promulgated thereunder (collectively, "Privacy Law"). When surveillance camera footage is recorded, resulting collections of data which include identifying information about individuals or information which enables identification of individuals (such as license plate numbers) are 'databases' which are subject to the Privacy Law. Database owners, holders and managers are subject to the applicable Privacy Law requirements with respect to such databases and the collection and use of database information, including, without limitation, use limitations, registration and data security requirements and data subject inspection rights. In addition, Section 11 of the Privacy Law requires provision of proper notice to individuals whose personal information will be included in a database. Consequently, appropriate signage must be provided so that individuals who object to being filmed can avoid access to the monitored premises if they prefer.

Practical Requirements

The Directive requires entities using CCTV systems to do the following:

1. Decision Making Requirements.

- Prior to implementing surveillance cameras in public spaces, evaluate the need for such technology and its effect on privacy and other rights, and consider less invasive alternatives.
- Ensure that the technology is implemented to achieve a proper purpose, that its use meets the proportionality test (that the benefit to be achieved exceeds the attendant invasion of privacy.)
- Exercise special caution when situating cameras in public spaces frequented by minors, such as schools and community centers.

2. Privacy by Design.

- Consider privacy concerns when designing the placement, coverage and functionality of CCTV systems.
- Limit coverage to relevant areas, utilize as few cameras as possible, and restrict filming to periods that are relevant to the desired purpose.
- Utilize image resolution that is appropriate for the desired purpose (for example, avoid a level of resolution that identifies facial features where such information is not needed).
- Exercise special caution where the following solutions are used: facial recognition or gait recognition software, monitoring activated by specific body language or dress, thermal or infrared solutions that record images in low-light environments, sophisticated tagging solutions having automatic searching capabilities or where CCTV footage is matched with other database information (such as biometric data).
- Voice recording must comply with the Eavesdropping Law- 1979.

3. Notices; Signage.

- Post clear, legible signs which notify individuals of CCTV filming both at the entrance to the filmed location and within the filmed area.
- Signs should preferably include the following: an image of a camera or other suitable image, the name of the responsible entity, the purpose of monitoring (for example, "security", "crime prevention", "traffic monitoring") and an Internet address containing the monitoring policy (see below) or alternatively a telephone number and email address for inquiries.
- Unless it would substantively harm the desired purpose of filming, post a "monitoring policy" on a designated website which identifies the following: camera location, responsible entity, description of filming capabilities, whether images are recorded, purpose of filming and recording, time period for which images will be retained, hours of filming, entity responsible for viewing and storing recordings, database manager and contact information for exercising data subject inspection rights.

4. Data Retention and Destruction.

- Evaluate whether live tracking suffices; record images only where necessary to achieve the desired purpose.
- Determine appropriate retention periods in light of the purpose to be achieved by recording and the sensitivity of recorded information. Ideally, the system should be designed such that images are automatically deleted once the retention period has expired.

5. Data Subject Inspection Rights.

- Database owners will not need to enable data subject inspection of surveillance images where the images are not processed to enable data subject identification (for example, using facial recognition software) so long as the images are not retained for more than 30 days.
- Data inspection requests must be specific and should be regarded with caution since other data subjects are likely to appear in the recorded images as well.

6. Data Security. Establish appropriate data security procedures, including limiting access to authorized individuals.
7. Use Restrictions. Use CCTV images only for permitted purposes, and disclose and transfer such images only in compliance with applicable law.
8. Outsourcing. Bear in mind that where a company outsources surveillance camera-related activities to third parties, the requirements of Directive 2-2011 on the Outsourcing of Data Processing Activities will apply.
9. Registration. In many cases, collections of recorded CCTV images will constitute databases that must be registered with the Israeli Database Registrar.

The full text of the Directive is available (in Hebrew) at: <http://www.justice.gov.il/NR/rdonlyres/FEDFC1AFDC-4586-B674-B2F1C935C14C/37913/42013.pdf>

Companies are advised to audit their existing processes and procedures to ensure compliance with the Directive, and to implement changes as necessary. Please feel free to contact Yoheved Novogroder (yohevedn@arnon.co.il) with any questions regarding the Directive or data privacy issues arising in the context of use of security or surveillance cameras.