



State Comptroller and Ombudsman  
Annual Report 70B | 2020

# Regulation of the Use of Biometric Databases

Abstract



# Regulation of the Use of Biometric Databases

## Abstract

### Background

“Biometrics” is a computerized technology that enables single-value identification of a person according to a unique human biological (anatomical or physiological) or behavioral characteristic through computerized evaluation. Identification and verification can be done in several ways such as face recognition, iris recognition, fingerprint recognition, walking recognition, voice recognition, palm recognition, and typing recognition. These properties are measurable and maintainable and can be used for verification and detection.

The increasing use of biometric applications<sup>1</sup> in the government and private sectors has many benefits, along with significant risks in information security and privacy protection aspects. These risks are even bigger when it comes to storing biometric information in databases. In light of this, the Israeli government has recognized the need for a comprehensive national policy in the field.

### Key figures

**4.5** million NIS

Images in the Ministry of Transport's driver's license database

**250,000**

Fingerprints in the identification system of employment seekers in the Israeli Employment Service - The Computerized System

**550,000**

Fingerprints and face photos in the database of foreign workers in the Population and Immigration Authority - Foreign Workers System

**5,500**

Voice samples in voice recognition database in telephone calls at the Prison Service - “Shahaf” system

**6.1** million NIS

Photos of 'Rav-Kav' transport card users stored in the National Transport Authority's databases and operators' databases for 4.5 million unique passengers<sup>2</sup>

November **2016**

The national policy for biometric applications was approved by the Prime Minister

<sup>1</sup> Biometric Applications - Taking biometric identifying measures, production of biometric identification data and use of biometric data.

<sup>2</sup> The number of images is higher than the number of passengers because in the past more than one multi-line card could be issued to the passenger.

---







---

## Audit Actions



 From March to September 2019, the State Comptroller's Office examined aspects related to regulating the use of biometric databases - the powers of the Biometric Identification and Applications Unit, the activity with regard to biometric databases in the governmental and private sectors, and the lack of use of the smart identity card. The audit was conducted at the Ministry of Justice - the Department of Privacy Protection and the Department of Legal Counsel and Legislation; the Government Computing Authority - the Government Cyber Defense Unit (the "Yahav"-Unit) and the E-Government Unit; and the Population and Immigration Authority, the Ministry of Transport and Road Safety, the Israel Police, the Israel Prison Service, Israeli Employment Service and National Public Transport Authority.

---

## The Situation Reflected in the Audit Findings

- 
- 
-  **Difficulties of the Biometric Identification and Applications Unit in fulfilling its mission:** Relying on voluntary supervisory and enforcement regulations and partial cooperation on the part of government bodies impaired the unit's ability to fulfill its mission according to the government's decision.
  -  **Database of drivers' licenses in the Ministry of Transport:** This database is defined as a high risk database. It was found by the unit that there is great risk to the biometric information stored in it in terms of information security and privacy protection. The Ministry of Transport has not yet provided the necessary professional response to mitigate the risk and has not yet arranged the use of this database for biometric quality images in primary legislation (including the transfer of information to other government agencies). This is despite the time period (14 years) since the Department of Justice recommended doing so.
  -  **Database of Immigrant Workers in the Population and Immigration Authority - Foreign Workers System:** As of July 2019, the Population and Immigration Authority has not yet completed the necessary actions to assess the system's compliance with the national policies for biometric applications. Moreover, for about 15 years, biometric identification information has been taken from foreign workers and stored in the system (to date, some 550,000 records), without the issue being regulated.
  -  **Voice recognition in telephone calls in the Prison Service - 'Shahaf' System:** In 2014, the High Court recognized the need to promote legislation on this issue and the Israeli Prison Service took action to promote it. However, legislation regulating the use of this means of identification has not yet been passed.
  -  **Image database of 'Rav-Kav' public transport card users:** The National Public Transport Authority does not have any information about the databases the public transport operators have, including information on the images in these databases.

This information is required for examining aspects of information security and protecting the privacy of passengers, and especially given their great sensitivity as they also include images of about a million minors. Moreover, the Biometric Applications Unit did not examine the issue and therefore lacked information regarding compliance of the aforementioned databases with the principles of the National Biometric Applications Policy.

-  **Examining Activity Regarding Biometric Databases in the Private Sector:** In a reality where there are hundreds of thousands of databases in the State of Israel, and the increasing use of biometric applications and their storage in databases, including in the private sector, the Privacy Protection Authority clearly does not have the ability to effectively monitor the operation of all existing databases in the State of Israel.
-  **Lack of use of smart ID card:** Smart ID cards have been issued since 2013 and although as of August 2019, 2.8 million smart IDs have already been issued, many types of government services (about 30) can also be obtained without requiring a smart ID and other means of identification. Furthermore, the data shows that the rate of use of the smart ID for obtaining available government services is extremely low. Therefore, in spite of all the benefits this has for government ministries and for residents, one of the aims for which the smart ID card was created has not yet been achieved - providing identified services based upon a very high level of authentication security.





Work Requirement Identification System - Employment Service (Computerized System): The Employment Service has received the Unit supervisor's certification that the system meets the national biometric application policy requirements.

The State Comptroller's Office commends the activity of the Biometric Identification and Applications Unit to examine the operation of biometric databases in government offices and their compliance with national biometric application policies and guidelines for its implementation.

The State Comptroller's Office commends the attempt to expand public transportation payment options by cell phone.

---

## Main Audit Recommendations

-  It is proposed that an examination be conducted in the National Cyber Security Authority regarding the unit's jurisdiction and powers and the tools at its disposal to fulfil its responsibilities. This is particularly the case with regard to the operation of government and public biometric databases and databases subject to government regulation (such as in local authorities, banks and hospitals), which are filled with sensitive information.
-  The Department of Transport should examine the findings of the unit, which led to its declaring the driver's license photo database a high-risk database, and undertake the necessary steps to reduce the risk.



Given the vast scope of data in the 'Rav-Kav' transport card users' databases, and because of the risks inherent in their operation, including their high sensitivity as well as one million photos of minors, the Biometric Identification and Applications Unit should consider examining the operation of these databases. It is also appropriate that the National Transport Authority should monitor the operation of these databases.



It would be appropriate for the Privacy Protection Authority to map the use of biometric databases in the private sector and carry out a risk assessment which will help to formulate a policy that will reduce the risks of privacy infringement in the preservation, processing and management of biometric information. It is also recommended that the findings from the mapping of the risks be brought to the attention of the Biometric Identification and Applications Unit, because it is the fulcrum of knowledge and experience in the biometric field, with a view to providing a comprehensive response to the risks.



It is recommended that the Population Authority and the Ministry of Transport, in collaboration with the Biometric Identification and Applications Unit, examine the possibility of consolidating the smart ID with the driver's license.



It is recommended that all government agencies holding databases that include personal information examine ways to improve information sharing between government agencies following the government's decision to adopt a policy whereby residents are asked for their information only once, to improve government service to the public and reduce the bureaucratic burden on citizens.

---

---









## Summary

The situation reflected in this audit report indicates a range of areas and issues that require corrective action: regulation of governmental biometric databases; ensuring that government databases follow national biometric policy, while minimizing the risks inherent in their operation; examination of the possibility for database reduction; examination and anchoring of the jurisdiction and powers of the Biometric Identification and Applications Unit; and the examination and mapping of the various risks inherent in the existence of biometric databases in the private sector and their violation of privacy, with the aim of formulating a policy that will reduce the risks.

Biometric applications and challenges in this evolving field will intensify over the years, requiring constant examination and control in order to manage risks and to protect the public effectively.



### Examples of biometric databases in the government sector

	<b>Population and Immigration Authority</b>	Database of Immigrant Workers - Maoz	550,000 fingerprints and face photos
	<b>National Biometric Database Authority*</b>	Smart national documentation – Passports and IDs	5.5 million face photos 3.8 million fingerprints
	<b>Israeli Employment Service</b>	Work Requirement Identification System - Computerized System	250,000 fingerprints
	<b>Ministry of Transport and Road Safety</b>	Driver's license photo database	4.5 million face photos
	<b>Israel Police**</b>	Database of suspects, defendants and convicts	1.3 million fingerprints 960,000 face photos 450,000 DNA samples
	<b>Airport Authority</b>	Automated border crossing – back of palm identification	1.3 million back of palm photos
	<b>Israel Prison Service</b>	Voice recognition system for telephone calls – Shahaf	5,500 voice samples
	<b>IDF**</b>	Database for identifying casualties, injured and missing persons	2.5 million fingerprints 1.1 million DNA samples

according to data collected during the audit, which the State Comptroller's Office processed.

\* For 4.5 million residents. It should be noted that saving the face image in the database is mandatory but keeping the fingerprints is not mandatory. A resident who agrees to keep their fingerprint in the database will receive documentation with a validity of 10 years, and a resident who does not agree will receive documentation with a validity of 5 years. For minors no fingerprints will be retained, so the documentation will be valid for 5 years (except for a minor over the age of 16 who can sign, in addition to one of his parents, on a consent to keep the fingerprints in the database). Also, as a result of requests for renewal of documentation, for some residents, more than one record is stored in the database.

\*\* Non-unique data - For some people in the database, more than one means of identification is stored.

