Unofficial Translation

Prohibition on Money Laundering (Rules for Conduct of Data Base and Protection of Information Therein) Regulations, 5762-2002

1. By virtue of the power vested in me under sections 28 and 32 (a) and (c) of the Prohibition on Money Laundering Law, 5760-2000\(^1\) (hereinafter “the Law”), after consultation with the Minister for Internal Security and with the approval of the Knesset Constitution, Law and Justice Committee, I hereby enact the following regulations:

**Chapter One: General Provisions**

**Definitions**

In these Regulations –

“reporting entity” – one of the entities that has a duty to report under section 7 of the Law as well as an entity that transmitted a report to the base, such report having been received under Chapter Four of the Law;

“the competent authority” – the Authority for Prohibition on Money Laundering, established under section 29 (a) of the Law;

“the data base” - the data base established under section 28 of the Law;

“information” – any datum or document received by the data base and by the competent authority, as well as any processing or result therefrom, including data and documents pertaining to the work methods of the competent authority, and including the actual existence of the information;

“computer”, “computer material” and “software” as defined in the Computers Law, 5755-1995\(^2\);

“Supervisor” - as defined in section 12 of the Law;

“computer records” – information in the computerized base of the Authority;

“original information” – information received from the reporting entity, whether included in the first report or whether it is supplementary information;

“supplementary information” – information within the meaning of section 31 (c ) of the Law;

“foreign authority” – an authority of the same nature as the Authority, located in another state;

“classified information” – information the disclosure of which is liable to endanger state security;

---

\(^1\) Sefer Ha-Chukkim 5760, p.293

\(^2\) Sefer Ha-Chukkim 5755, p. 366
Unofficial Translation

“Israel Police” – a person empowered by the General Commissioner of the Israel Police for that purpose;

“General Security Service” – a person empowered by the Head of the General Security Service for that purpose;

Safeguarding of Information – General Principles

2. (a) The rules and procedures under these regulations relating to security measures shall not detract from the provisions of the Public Bodies (Safeguarding) Law, 5758-1998\(^3\); in these regulations, “security measures” shall be understood as defined in section 1 of that Law.

(Two) Rules and procedures relating to classified information, classification of posts and security screening shall be in accordance with the guidelines of the General Security Service

(Three) Rules and procedures relating to information transmitted to the competent authority by the Israel Police shall be in accordance with the guidelines of the Israel Police

(Four) Any information transmitted to the Authority by the Israel Police or by the General Security Service shall be considered classified as “top secret” unless classified otherwise provided by those entities.

Chapter Two: Conduct of Data Base

Rules and procedures for conducting base and information therein

3. Without derogating from the provisions of Regulation 2, the Head of the Competent Authority shall prescribe rules and procedures dealing inter alia with the following:

(1) the mode of peripheral and internal security of the premises of the Authority and of the computers on its premises;

(2) safeguarding of the communication infrastructure;

(3) safeguarding of computer material that serves the base and the computers belonging to the Authority, or is located therein;

(4) classification of information and documents in the Authority’s possession, authorization of access by the Authority’s employees and those acting on its behalf and in its service, and rules for compartmentalizing of information;

---

\(^3\) Sefer Ha-Chukkim 5758, p.348
(5) mode of keeping records, whether in documentary form or as computer records;

(6) dealing with alarm signals regarding irregular occurrences in the base, including during the process of absorbing information, unauthorized transmission or use of information, as well as any attempt to perform unauthorized acts in the computer or with computer material;

(7) mode of requesting supplementary information;

(8) transmission of information under section 30 of the Law, in a manner that prevents exposure of information, its distortion or damage thereto during the transmission process, including the manner of safeguarding of electronic transmissions.

Classification of information and authorization of employees

4. (a) Without derogating from the provisions of Regulation 2, the Head of the Authority shall determine the classification of information in the base and the authorization of employees to examine and process information, including compartmentalizing action among employees in accordance with their functions; in this chapter “employees” shall include a contractor, a contractor’s employees and temporary employees of the competent authority.

(Two) Access, examination and treatment of information received from the Police or a foreign authority which has requested preservation of confidentiality, shall be limited exclusively to the Head of the Competent Authority and additional employees who have received special authorization from the General Commissioner of the Israel Police.

(c) Access, examination and treatment of classified information shall be limited exclusively to the Head of the Competent Authority and holders of classified posts.

Information included in application to receive information

5. (a) Information received by the competent authority from the Israeli Police or from the General Security Service shall be stored in the data base in a manner that prevents access thereto from any external communication source and prevent its examination or treatment by any unauthorized sources as stated in Regulation 4 (b) above. For this purpose, the competent authority shall act in accordance with the guidelines of the Israel Police and the General Security Service, as stated in Regulation 4 (b) and 4 (c).

(b) Information included in an application to receive information under section 30 shall not be transmitted to any sources either within the State or outside thereof except with the consent of the entity that included the information in its
Unofficial Translation

application; this provision shall not apply to an application of a foreign authority in which confidentiality was not requested.

(c) Where an application to receive information was filed by one of the entities specified in section 30 of the Law, the competent authority shall not approach any sources either within the State or outside thereof, in any matter pertaining to the application, unless having first received the consent of the source from which the application was received; this provision shall not apply to an application of a foreign authority in which confidentiality was not requested; consent for purposes of this regulation may relate to a specific application or a particular kind of referral or source; for purposes of this sub-regulation, “referral” shall include entry into a computerized data base, which records all acts performed therein.

(d) Subject to the provisions of the Legal Assistance Between States Law, 5758-1998, the competent authority shall take measures for protection of the confidentiality of information received from a foreign authority within the framework of the Law, if that the authority has so requested.

Chapter Three: Rules and Procedures for Safeguarding of Data Base and Information Therein

Principle of Completeness of Original Information

6. All original information, including computer records that contain original information that was transmitted to the competent authority by a reporting entity, shall be kept with the Authority or in the computers of the Authority, without any alterations; recording of remarks, alterations or additions, including cancellation, archiving or elimination of computer records from the data base shall be effected without impairing the completeness, reliability and correctness of computer records that contain original information.

Choice of Infrastructures for Computerizing System and Operating Software

7. In the infrastructures of the computerization system and operating software at the base, the requirements of the Standards for Safeguarding of Information Systems, determined in accordance with Israeli Standard T.I. 7799 and International Standard ISO-15408 shall be complied with; the computerization system and operating software shall comply with the requirements laid down in these regulations for systems with a high classification that contain computer material and are conducted on a number of levels of security classification and access authorizations.

Assurance of Computer Availability

8. The configuration of computers that serve the data base shall ensure a high level of availability, stability and reliability in order to prevent a local system failure.
Separation of Computerization Systems

9. (a) The base shall consist of a number of separate computer systems, including the following:

   (1) a computer for collecting information and communication with the reporting entities, national databases, the Israel Police, the General Security Service and foreign authorities;

   (2) a research computer, which contains and maintains the database;

   (3) a computer system for communication by way of internet or another system of the same category.

(Two) The collection and research computers shall be connected for the purpose of transmission of information by way of a dividing network that creates galvanized insulation between these computers and that monitors the contents of messages transmitted between the computers; the dividing network shall form a barrier of hardware and software between the collection computer and the research computer.

(Three) There shall be no connection whatsoever between the research computer and the public communication network other than by way of the collection computer.

(Four) The Head of the Authority may, for purposes of receiving information from a reporting entity or other entity, approve the connection of the collection computer to those entities via the public communications system of “Bezeq” Israel Telecommunications Company Ltd., or of another operator. The connection of the collection computer to the Israel Police or to the General Security Service shall be effected with the consent of those entities.

Safeguarding of Communication Lines

10. An internal communication system of the Authority’s computers shall be installed in accordance with the principles of safeguarding prescribed in Regulations 7 and 9 and shall ensure, inter alia protection against electromagnetic leakage or leakage of a radio frequency, all in order to prevent unauthorized listening or penetration of the base; the Head of the Authority, after consultation with the Supervisor may provide that the internal communication lines shall operate via the public communication channels, which are safeguarded by encryption and special software systems.

Safeguarding of Collection Computer

11. The divisions of the collection computer network which provide the maintenance of the electronic connection between the entities reporting as required by law and the authorities legally entitled to receive information as well as the connection with other
national data bases, shall be protected by means of software and a protection system from unauthorized entry and introduction of hostile software.

Backup for Computerization and Information Systems

12. The computerization and information systems shall be backed up in the manner and form prescribed by the Head of the Authority in order to ensure the continuity of regular functioning and the completeness and reliability of the computer material, even in case of a physical or logistic malfunction in the components of the computerization and communication systems, or a physical harm to the premises in which the base is located.

Maintenance of Computerization and Communication Systems

13. Preventative maintenance, repairs, additions and technological updating of the computerization and communication systems shall be performed regularly, promptly and skillfully by the technicians and engineers of the service suppliers, who have been approved in advance by the Head of the Authority or on his behalf; these activities shall be performed without the technicians or engineers involved having any access to the contents of the computer records in the data base; where it is not possible to perform these activities without such access to contents, the activities shall be performed under the physical supervision of an authorized worker of the Authority.

5762
(2002)

Meir Shetreet
Minister of Justice