Name of Regulation: Privacy Protection

This version is an English translation of the Regulations published in Hebrew on the University's web-site. In the event of contradiction or inconsistency between this English version of the Regulations and the Hebrew version, the latter will prevail.

1. Chapter 1: Goal

Tel Aviv University is committed to protect privacy and provide data protection, including the privacy of its employees, students, whoever enters its gates, and whoever has any other research or administrative connection to it. This regulation is intended to assert the University's policy regarding the aspects of these matters, by aiming to strike an appropriate balance between privacy interests and other University interests, such as promoting research and academic freedom, security, public order, and efficient management.

While the University, like any organization, is subject to Israeli law, there are unique aspects characterizing an academic institution with the principle goals of *producing knowledge, preserving it, and imparting it on behalf of the public for perpetuity*. By virtue of being an entity that considers itself an intellectual and ethical engine, in Israel and worldwide, the University has undertaken to apply rules for protecting privacy beyond what is required by Israeli law, and as specified in this regulation.

2. Chapter 2: Definitions

"The University"	Tel Aviv University.
"The Committee"	The Committee named in section 3.3 below.
"The PPA"	Protection of Privacy Act 5741-1981, or any law that should replace it.
"The manager"	Whosoever is appointed by the University as a database manager.

"The database"	Database of the University.
"personal data"	Data regarding an identified individual, or an individual identifiable by reasonable means, directly or indirectly, from the data itself or in connection with other data, in relation to his or her personality, his or her body, his or her lifestyle, the status of his or her health, his or her financial status, his or her beliefs and opinions, and his or her habits, including identification number, biometric information, and any other distinct means of identification.
"Database"	A database is defined by the PPA as a collection of personal data, stored digitally, including magnetically or optically, and enabling computerized processing.
"Database owner"	Tel Aviv University
"Database controller"	Whosoever has a database in his possession on a permanent basis and is authorized to make use of it.
"privacy violation"	Any use of information prohibited by law or by this regulation, including collecting information and processing it.
"human-subject research"	Any research in which human beings are involved, including human material or personal data about human beings, including such as are conducted in the framework of studies for different degrees.
"Chief Information Security Officer"	The University appointee for information and cyber protection (CISO).
"Data subject"	The person who is the subject of the personal data and to whom the data relates.

3. Chapter 3: Officials

3.1. Data Protection Officer:

1) The University will appoint a Data Protection Officer (hereafter the DPO) who will hold the highest authority for directing matters of privacy at the University. The DPO will be independent in his decision-making and in the execution of his position.

2) The DPO will be experienced and familiar with the diverse units of the University, and have background or training in the field of privacy. The DPO will not fill other positions that might place him or her in a conflict of interests. As a rule, the DPO will be a tenured, senior member of the academic staff. The appointment of a DPO who is not a senior academic staff member requires an explanation.

3) The DPO will be appointed by the Management of the University and will submit an annual activity report on the subject to the Management of the University and to the Senate. The term of the appointment is two years, and may be extended for up to three consecutive terms (a total of 6 years).

4) The DPO will not be removed from his or her position during the term of appointment unless by a substantiated decision of the Management of the University which will be approved by the Executive Council.

5) The resources required to fulfill the position will be made available to the DPO.

6) The DPO will have the authority to investigate and receive access to any information in the University required for the purpose of fulfilling his or her role.

3.2. The duties of the DPO:

1) To lead the University policy on issues of privacy and to oversee their implementation, including providing instructions to various University units and entities in this field.

2) To ensure coordination between the University bodies in charge of executing privacy protection.

3) To alert the Management of the University to deviation from this regulation.

4) To make decisions where exercise of judgement is required, while ensuring the appropriate balance between academic freedom and strictness of privacy, and subject to the letter of the law.

5) To represent the University to relevant external parties in all matters relating to privacy.

6) To execute the duties of the DPO in accordance with the law.

7) To raise awareness and conduct instructional activities in his or her field of responsibility.

8) To serve as the organizational address for the purpose of accepting inquiries on issues of privacy protection and to forge the connection with the relevant privacy protection authority.

3.3. The Committee for Privacy Protection:

3.3.1. Composition of the Committee

The Committee for Privacy Protection is hereby established, and its composition is as follows:

The Data Protection Officer - Chairperson

A senior academic staff member who is an active
Researcher in fields relevant to the subject of privacy,
Who will be appointed by the Rector - Member

Director of the Research Authority or his or her representative - Member

Chairperson of the Ethics Committee or his or her representative- Member

Chief Information Security Officer or his or her representative - Member

The Legal Advisor or his or her representative - Member

The Committee will determine its working agenda.

3.3.2. The duties of the Committee

3.3.2.1. To assist the DPO in providing advice to the Management of the University and to the Executive Council in matters specified in this regulation;

3.3.2.2. To propose changes and amendments to this regulation and to other relevant regulations;

3.3.2.3. To examine the existence of compatibility between working regulations of the relevant units as specified in Chapter 5 below, and to advise the DPO on the subject;

3.3.2.4. To deliberate on cross-organizational matters in the field of privacy protection;

3.3.2.5. To fulfill the duties of the Committee for transferring information among public bodies according to the Privacy Protection Act, as per the authorization by the Director General of the University.

3.4. Officer responsible for Rights of Data Subjects

In coordination with the DPO, the Director General of the University will appoint an administrative employee who in addition to his position will be responsible for inquiries from subjects of data, in accordance with the provisions of Chapter 6 of this regulation. The responsibility will be professionally subordinate to the DPO, and administratively to the Director General, and will follow their instructions.

4. Chapter 4: The principles of privacy protection at the University

4.1. Principles

4.1.1. The University will collect personal data and process it, while abiding by the law and relevant rules, according to ethical principles of research, and other University regulations, with preference for collection of anonymous data, according to the circumstances, and to the extent possible.

4.1.2. Collection and processing of personal data will be conducted with fairness, in respect of the rights of the data subjects, with transparency, and for accomplishing legitimate and legal purposes related to the University's activity, as well for its efficient and proper management, and to an extent no greater than is required to achieve these purposes.

4.1.3. University units and all University employees in the framework of their positions, are required to avoid violating a person's privacy without his or her consent. In case of doubt, the employee will refer to his or her superiors for instructions, and if required, the superiors will seek the opinion of the DPO as per this regulation, for the purpose of reviewing the issue and providing suitable instructions.

4.2 Purposes of collection and processing of personal data

4.2.1. The personal data collected and processed by the University and on its behalf will serve it for these purposes:

a. For the purpose of approaching and providing appropriate information for candidates and their registration as students in various study programs; management of all aspects of students' studies, and contact with alumni;

b. For the purpose of research in any field of knowledge and by any valid method of scientific research, including collection of personal data, its processing, whether in an identifiable manner or not, and retaining the data as per the research needs;

c. For the purpose of managing the University, including human resources management of all personnel, meeting contractual agreements with donors and other third parties, and with respect to activity of those who are not students or people working with the University or on its grounds;

d. For the purpose of abiding by the instructions of the Law, court orders and certified authorities.

e. For any other appropriate purpose, with the data subject's consent.

4.2.2. Personal data collected for one purpose will not be used for another purpose unless by consent of the data subject, or on the basis of another purpose among those specified in this section, which permits such use.

4.3. Obligations of the University

4.3.1. The University will act with respect to privacy and data protection in accordance with the instructions of the law and regulations of research foundations, which apply to its activity, according to the circumstances.

4.3.2. The University will use personal data collected only for an appropriate purpose in accordance with this regulation.

4.3.3. The University will receive the consent of the data subject in advance, subject to the instructions of the law regarding the collection of personal data and its intended processing, will notify the subjects whether there is a legal obligation to provide the data, and whether the personal data will be transferred to another party. The notice will also include information regarding rights of a data subject related to the personal data about him or her.

4.3.4. The University will not transfer personal data collected to third parties unless the data subject consents, or if it is required or permitted by the instructions of any law, and subject to this regulation.

4.3.5. The University is bound to acting to protect the confidentiality of personal data and its security according to the kind of data, its sensitivity and magnitude, and as is customary in the field of information security.

5. Chapter 5: Responsibility and mechanisms for applying the principles

General

All University entities, including its units, employees, students, suppliers, visitors, and guests are subject to the instructions of this regulation. All University regulations and instructions will be implemented and interpreted according to this regulation.

5.1. Information security

1) The University, data processors and controllers of databases at the University are obligated to protect information security in accordance with the level of security required by law for said database, and in accordance with Tel Aviv University's regulations on information security and the contracts to which they are subject.

2) Any party at the University which controls a database must report it to the CISO by using these forms:

   For research databases – The form in Appendix A1 to this regulation must be completed.

   For administrative databases – The form in Appendix A2 to this regulation must be completed.

3) The University, by means of the CISO, will set regulations and instructions regarding information security at the appropriate level, as per the degree of sensitivity of the data saved in them, the size of the databases, and according to accepted technological standards, all subject to the requirements of the law.

5.2. Research

The University is committed to the existence and prosperity of research under principles of academic freedom, along with its commitment to data protection. Administrative units that assist researchers in their research should facilitate research while adhering to the rules of privacy protection. Nevertheless, situations may occur whereby exercise of judgment is required to find the suitable balance between research requirements and privacy requirements. In such cases, one should refer the matter to the DPO who has the authority to decide.

Commitment to research ethics: Any research of human subjects, including research that uses questionnaires and interviews, requires the permission of the University Ethics Committee, according to the binding rules of ethics with respect to experiments with human subjects. The subject of privacy is part of the requirements in submitting a request for permission for research to the Ethics Committee, and abiding by the terms of privacy protection is a condition for receiving this permission. As part of the research submission system, the requesters must relate to questions concerning the potential for violating the privacy of the research subjects, and to verify the required manner of handling information as specified in section 5.1., with the Data Protection Officer.

Commitment to privacy in funded research: Academic research activity financed or supported by an entity external to the University, from Israel or abroad, is likely to include additional obligations regarding privacy protection and information security. In the event that this activity includes collecting or processing personal data, one must contact the Research Authority to assure abidance by binding rules prior to beginning any activity related to the information.

Commitment to privacy protection in transferring data among research entities: The transfer of data among researchers and research entities outside of the University requires an arrangement as specified in section 5.5.1.

5.3. Privacy in digital University devices

The University will monitor University data stored in digital devices under its ownership, including devices in which personal data is stored, subject only to this regulation and the following principles:

(a) Legitimacy – limitation of tracking and use of data produced as a result of it, for purposes vital to the activity of the University;

(b) Proportionality – the means used should be those which will harm privacy the least;

The monitoring is subject to adopting a binding instruction that will regulate, inter alia, the manner of monitoring while avoiding exposure of personal data stored in the devices.

5.4. Camera use

Generally, camera use on campus will be in accordance with the provisions of any law, and in abidance with the principles of privacy protection.

5.4.1. Camera use for security purposes will be subject to that stated in the *Security Cameras Regulation*.

5.4.2. Camera use for research purposes will be with the authorization of the Ethics Committee.

5.4.3. Camera use for teaching purposes will be subject to this regulation.

5.4.4. Camera use for work purposes will be subject to this regulation.

5.5. Transfer of personal data

Transfer of personal data among entities, when needed, shall comply with privacy protection. **Instructions for transfer of personal data in a number of common situations** are specified below:

5.5.1. Transfer of personal data for research purposes

Research material transfer agreements (MTA) including data transfer agreements (DTA), which include personal data, for which the Vice President for Research and Development is responsible, will be in accordance with the rules specified in: https://research-vp.tau.ac.il/import-export.

5.5.2. Transfer of personal data for outsourcing

Transfer of personal data to a third party and its processing requires preliminary examination of information security risks in connecting and setting explicit contractual instructions on subjects such as purposes for use of information, type of processing, duration of the contract, manner of returning the information upon concluding the agreement, etc. Every researcher or unit interested in contracting with a third party must perform the actions stated above and document the preliminary examination stated above, and confirm with the Supply Unit, and to the extent necessary with the Office of the Legal Advisor, that the agreement with the same third party will include the appropriate contractual instructions.

5.5.3. Transfer of personal data between public bodies

Any University entity seeking to transfer personal data to a public body or to receive personal data from such a body will apply to the Privacy Protection Committee with a formal request, with all details completed, on the request form for receiving personal data from a public body according to the Privacy Protection Act (form A) attached to this regulation. Only after the committee has approved the request, will the form be circulated for the signatures of the appropriate officials.

6. Rights of data subjects

The data subjects have rights by law and as specified in this regulation. Data subjects may seek to exercise their rights as specified below. Applications will be referred to the person responsible for the rights of data subjects, as specified in section 3.4. above.

6.1. The right to access – a data subject is entitled, upon request, to receive an answer whether the University holds personal data about him or her, and to the extent that such personal data exists, he or she is entitled to receive a copy of that data. The data subject is entitled to receive details regarding the source of the personal data about him or her, the legal basis which served for collecting the data and processing it, the purposes of the collection and processing of the data, and the planned duration of saving the data, who holds the data, and what are his or her rights in relation to the data. This right will not apply in relation to personal data which the University is prohibited from transferring to the data subject in accordance with the provisions of any law.

6.2. The right to rectify personal data– to the extent that the personal data held by the University is not precise, the data subject is entitled to request its rectification, subject to other instructions that are likely to apply to the data.

6.3. The right to deletion of personal data– a data subject is entitled to request deletion of the personal data regarding him or her held by the University, if one of the following terms applies:

- When there is no longer need for the data for the purposes for which they were collected;
- When the processing is done on the basis of the data subject's consent, and he or she retracts this consent;
- When the personal data has been attained or processed in an illegal manner or contrary to this regulation;
- When the law requires deletion of the data.

The University will delete the personal data, unless it has a legitimate interest, or legal, ethical, social, or professional obligation not to do so, or reason in executing its regular functions in the course of its regular work.

6.4. The right to limit use of the personal data– a data subject is entitled to request that the University limit the use of personal data about him or her, in the following instances:

- If the data subject has requested rectification of the data, and as long as this request is under consideration by the University;
- If processing the personal data is contrary to the instructions of the law or this regulation;
- If the purpose for which the personal data was collected has been fulfilled, yet there is a legitimate purpose for the data to be retained by the University.

6.5. The right to object to use of personal data– if the processing of the personal data was not done on the basis of informed consent, but rather on another legal basis, the data subject is entitled to request that the University ceases collecting and processing the personal data about him or her. Such a request will be considered by the DPO, in light of the instructions of the law, and with attention to the legitimate interests of the University.

6.6. Data portability– a data subject is entitled to receive a copy of the personal data about him or her in a known format, and is entitled to request its transfer to another entity. The request, as stated, will be examined by the University in light of the instructions of the law, and according to the technological possibilities. This right will not apply in cases in which the processing of the personal data is required for the purpose of protecting public interest.

The exercise of this right does not prevent the University from continuing to use the personal data about the data subject in cases in which it is permissible in accordance with the instructions of any law, and in order to actualize a legitimate interest (a valid purpose) of the University, or a legal, ethical, social, or public obligation.

6.7. The right to retract consent – to the extent that processing the personal data is based on informed consent, the data subject is entitled to retract this consent at any time. The right to retract will apply from the time of receiving the notice at the University, and without diminishing from the legality of processing the personal data already conducted prior to receiving the notice of retraction of consent.

6.8. The right to object to the creation of a behavioral profile – a data subject is entitled to object to processing the personal data for creating a behavioral profile of him or her by means of the processing of personal data, except in one of the following cases:

- Based on the specific circumstances related to the case, when the basis for collecting personal data is the public interest or another legitimate interest of the University;

- In cases in which the service provided is an online service;

- When the purpose of creating the profile is scientific research, historic research, or for purposes of statistics, based on the specific circumstances related to the case,

and this is in cases in which processing of the personal data is essential to executing the task at the base of which lies the public interest.

6.9. The right to object to automatic decision-making procedures – when processing personal data has legal implications or other significant implications for the data subject, the data subject is entitled to object to the products of personal data processing automatically conducted about him.

6.10. Submitting a complaint – a data subject is entitled to submit a complaint to the DPO regarding use of information about him and its processing.

7. This instruction applies from the date of its publication and replaces the previous instruction from December 3, 1987.

Privacy protection regulation 01-014 [226365]
February 2, 2021

נהלים /הצעות /הגנת הפרטיות נוהל 01-014 [226365]
2.2.2021