

Appendix
to Directive No. 6.18.1-06/1801-01
of the State University
Higher School of Economics
dated January 18, 2011

APPROVED
by Directive No. 6.18.1-06/1801-01
of the State University
Higher School of Economics
dated January 18, 2011

Procedures for Protecting Personal Data of Employees of the State University Higher School of Economics

1. GENERAL PROVISIONS

- 1.1. The present Procedures have been developed in compliance with the requirements of Russian legislation in order to protect the personal data of employees of the State University Higher School of Economics from unauthorized access, unlawful use, and loss.
- 1.2. Personal data fall into the category of confidential information. Their confidentiality may be waived if they are depersonalised, once the retention period of 75 years has passed, or in other cases stipulated by Russian legislation.
- 1.3. For the purposes of this document, the following definitions are used:
 - Employer or the University – State University Higher School of Economics
 - Employee – an individual who has entered into labour relations with the Employer
 - Personal data – any information that refers to an individual (subject of personal data) identified or identifiable by this information, individual (subject of personal data) directly or indirectly identified or identifiable, including his/her last name, first name, middle/patronymic name, date and place of birth, address, marital, social or financial status, education, occupation, income and other information
 - Processing personal data – any action (operation) or a sequence of actions (operations) involving personal data, whether by automatic means or not, including collection, recording, systemization, accumulation, storage, specification (updating, changing), retrieval, use, transfer (dissemination, granting access), depersonalisation, blocking, removal, and destruction of personal data
 - Confidentiality of personal data – provision binding upon any authorised individual who has been granted access to personal data of employees, and requiring the protection of data from unauthorised disclosure without employees' consent or other lawful grounds.
- 1.4. The present Procedures are binding upon all employees of the University.

2. PROCESSING PERSONAL DATA

- 2.1. The University determines the scope and composition of employees' personal data to be processed on the basis of the provisions of the Constitution of the Russian Federation, the Labour Code and other federal laws of the Russian Federation.
- 2.2. The personal data of employees shall be processed only for the following purposes:



- Observance of Russian legislation
- Assisting employees in recruitment, training and professional advancement
- Ensuring the personal safety of employees
- Controlling the quality and quantity of the work performed
- Ensuring the safety of property belonging to employees and the employer.

2.3. No transmission of an employee's personal data without his/her consent for further commercial use is allowed.

2.4. The employee's personal data shall be obtained solely from himself/herself unless such data can only be obtained from third parties.

2.5. An employee's personal data shall be obtained from third parties only if the employee is duly notified and gives his/her express written consent.

The notification regarding the obtainment of an employee's personal data from third parties shall stipulate the following:

- Purpose of obtainment of the personal data
- Expected sources and methods used to obtain personal data
- Nature of personal data to be obtained
- Possible consequences of the employee's refusal to agree upon the obtainment of the data.

2.6. The employee whose personal data was requested must be notified about the transmission of his/her personal information to third parties unless such notification is impossible by virtue of force majeure circumstances, such as natural disasters, accidents and catastrophes.

2.7. When transmitting an employee's personal data to third parties, the employer must warn such parties that this data can only be used for the specified purposes and must require a confirmation that these requirements were duly observed. The parties that obtain an employee's personal data must follow the information security (confidentiality) procedures. This provision is not applicable to the exchange of employee's personal data as set down by the Labour Code of the Russian Federation or other federal laws.

2.8. The University is not entitled to obtain and process an employee's personal data regarding his/her political, religious or other beliefs and private life.

Following the provisions of Article 24 of the Russian Constitution, the University has a right to obtain and process an employee's personal data regarding his/her private life in cases directly connected with labour relations only with the employee's written consent.

The University is not entitled to obtain and process personal data regarding the employee's membership in public associations and union activities unless it is required by the Labour Code of the Russian Federation or other federal laws.

2.9. No request of private information regarding an employee's state of health shall be allowed unless it pertains to the employee's ability to perform his/her professional duties.

2.10. Personal data in paper form shall be transferred to the archive upon expiration of its retention period. The processing of documents transferred for archiving shall be performed by the Administration and General Services Office of the University.

3. ACCESS TO PERSONAL DATA

3.1. The following University staff members have access to personal data of the employees:

- Rector
- President



- Academic Supervisor
- First Vice Rectors
- Vice Rectors
- Director for Finance
- Chief Accountant
- Director for Administrative Affairs
- staff of Human Resources Office
- staff of Accounting Office
- staff of Planning and Finance Office
- staff of IT Office
- staff of Legal Support Office
- staff of Administration and General Services Office
- staff of Office of Online Media Resources
- staff of Security Office
- employees who were duly authorized by the Rector or Director for Administrative Affairs to obtain and process personal data of employees

3.2. Employees listed in Article 3.1 have access only to such personal data that are required for the due performance of their professional duties.

4. PERSONAL DATA PROTECTION

4.1. Personal data protection is a complex of measures against possible violations of accessibility, integrity, authenticity and confidentiality of personal data that assures reliable security of information in the course of University operations.

4.2. Protection of employees' personal data against unlawful use or loss shall be provided at the expense of the employer following the procedure established by the federal law.

4.3. Organisation and monitoring of personal data protection shall be ensured by the heads of University subdivisions and authorized personnel with access to such personal data.

4.4. The following data shall be protected:

- Employees' personal data
- Documents that contain employees' personal data
- Electronically stored personal data

4.5. Protection of information stored in electronic databases of the employer from unauthorized access, distortion and deletion as well as from other unlawful action shall be ensured through the differentiation of user access rights through user accounts and password system.

4.6. The storage of personal data in the University shall be organised in such a way as to exclude its loss or unauthorized use.

4.7. To ensure protection of personal data kept by the employer, employees have the right to:

- Obtain full information on their personal data and its processing (including automatic processing)
- Obtain free access to their personal data including copies of any records made with use of personal data unless otherwise stipulated by federal law
- Appoint representatives for further protection of their personal data
- Obtain access to appropriate medical information through corresponding healthcare specialists of their choice
- Demand the deletion or correction of invalid or incomplete personal data, as well as data processed in violation of the Labour Code of the Russian Federation or any other federal law. If the employer



refuses to correct or delete such personal data, the employee shall be entitled to notify the employer in writing on his/her disagreement with relevant grounds for such disagreement. The employee has the right to add his/her own opinion to personal data involving assessment of the employee.

- Demand that the employer notify all parties to whom invalid or incomplete personal data was communicated about the relevant corrections, revisions or deletions made to such data
- Appeal to court against unlawful actions or inaction of the employer while processing or protecting employees' personal data.

4.8. In order to regulate staff access to the confidential data, documents and databases of the University and protect data from unauthorized access, the management responsible for personal data processing shall comply with and ensure:

- Limitation and regulation of the list of employees whose duties require access to personal data
 - Clear, selective and rational distribution of documents and information among staff
 - Rational arrangement of staff workplaces which eliminates uncontrolled use of protected information
 - Understanding of regulations on information security and protection of privacy safety by the staff
 - Availability of necessary conditions in the office for processing confidential documents and databases
 - Authorisation and regulation of employees with access to information databases with personal data
 - Adequate information destruction procedures
 - Due detection of violations in the access authorization systems
 - Adequate measures against accidental loss and disclosure of information while processing confidential documents
 - Limitation of access to documents that contain personal data of employees

4.9. For the purpose of personal data protection in the University, the following regulations shall be met:

- Procedures for admitting, registering and monitoring visitors
- Entry by ID cards
- Accountability and monitoring of ID cards distribution
- Security equipment and alarm system
- Territory, building, premises and vehicle security arrangements
- Confidentiality requirements for job interviews

4.10. All confidentiality measures for collecting, processing and storing personal data are applicable to both paper and electronic (automated) media.

5. LIABILITY FOR VIOLATING RULES REGULATING THE PROCESSING AND PROTECTION OF PERSONAL DATA

5.1. Employees that violate rules regulating the processing and protection of employees' personal data as stipulated by the applicable Russian legislation and the present Procedures shall be liable in accordance with the applicable Russian legislation.

5.2. An employee who provides false documents or false information about himself/herself shall be subject to disciplinary action as stipulated by the Labour Code of the Russian Federation.

