OFFICE OF THE PERSONAL DATA
PROTECTION INSPECTOR

Recommendations Regarding Personal Data Protection in Labor Relations

Goal of these recommendations is to establish high standard of personal data protection in employment and labor relations, to protect rights of data subjects (employees), to raise awareness of data controllers (employees) regarding the issues of personal data protection, and to prevent improper and/or inconsistent interpretation of the law.

The recommendations are prepared on the basis of Georgian Legislation[1], Recommendation of the Committee of Ministers of the Council of Europe (89)2[2], recommendations of International Labor Organization[3], decisions of the European Court of Human Rights[4] and best practice of European countries[5].

1. Definition of Terms

For the purpose of this guidance, used terms will have the following meaning:

1. ***„Employee" includes:***

- **Applicant / candidate –** person, who applied to the employee with the purpose to get employment;
- Employee – person who has labor relations with the employer or carries out paid activity in budget institution, including non-staff servant.
- Person on an employment reserve list;
- Intern, volunteer;
- Also, all other persons who had any of the above-mentioned relations with the employer.

[1] Constitution of Georgia, 24.08.1995; Law of Georgia on Personal Data Protection, 28.12.2011; Organic Law of Georgia - Labor Code of Georgia, 17.12.2010; Law of Georgia on Public Service, 30.10.1997.
[2] Rec (89) 2 on the Protection of Personal Data Used for Employment Purposes – Committee of Ministers, Council of Europe, 18.01.1989
[3] Protection of Workers Personal Data – International Labor Organization; International Labor Office Geneva, 1997;
[4] ECHR, Halford v United Kingdom; Copland v United Kingdom; Niemitz v Germany;
[5] UK, France, Ireland, Latvia.

2. ***"Labor relations"*** mean relation between the "employee" and the "employer", which includes pre-contractual, contractual and post-contractual relations, as after termination of labor relations, personal data of former employees are kept at the employer for some time.

2. General Principles

Personal data protection ensures balance between employer's legitimate interests and rights of the employee. In labor relations, personal data protection does not mean restriction on collection and procession of the data required in an employment process.

Personal data includes any document produced by the employer about the employee, for example – copies of ID cards, copies of education or qualification certificates, CV, letters of reference, medical-drug certificates, test results, photo, e-mail, etc.

In employment and labor relations, personal data may be processed for different reasons; for instance: selection of qualified staff, execution of labor contracts, improvement of staff qualification, protection of organization's security and property; employees' health insurance and etc.

In terms of labor relations, data controller (employer) is obliged to observe the following principle:

- **Respect for constitutional rights of a person** – in terms of personal data processing, the employer should respect constitutional rights and freedoms of the employees, including honor and dignity, privacy and development rights. At workplace, the employee has to have the chance to establish social and personal relations. Information that is not related to professional operation, *for instance, hobby, friends, preferred sport or cultural activity, may be processed by the employer only on the basis of employee's consent, though such data should not be used as a decisive factor for hiring, career promotion and payroll.*

- **Fair and legal processing of personal data** – the employer must process the employee's data in compliance with legal requirements and must maintain equal and fair treatment towards all employees. *For instance, different sets of data should not be collected from persons holding identical positions.*

- **Non-discrimination** – personal data processing should not aim at or result in any form of discrimination in hiring, labor relations and career promotion processes.

- **Awareness of employees –** the employee must have information about legality of his/her personal data processing (purpose, grounds of data processing; whether such data are transferred to third parties, etc.) and his/her rights.

- **Adequacy and proportionality** – each case of data processing (gathering, storage, disclosure, etc.) must have a separate, legal, and clearly defined purpose. In terms of labor relations,

employer must process only those personal data, which are necessary for achievement of the purpose.

3. Practical Aspects of Personal Data Processing

3.1. Gathering of Personal Data

Employee's personal data must be collected from the employee himself/herself, and in case if it is necessary to collect such information from the third party, the employee must be informed about it – must be explained about the purpose and reason of collecting the personal data from the third party, possible source of information, and the way of gathering. Unless it is otherwise prescribed by the law, collection of information from the third party is possible only on the basis of advance and informed consent of the employee.

In light of proportionality and adequacy principle, the employer must gather only those personal data that are necessary for selection of the candidate and for labor relations, in consideration of job specifications. During the hiring process, only those data must be gathered, which are necessary for selection of qualified candidate. Questions asked during the interview and collected personal information must be adequate to the purpose of selecting qualified person for the specific position.

If employee provides employer with information that is not necessary for labor relations, the documents must be returned to data subject or must be destroyed in accordance with established rule.

If the applicant is required to fill in the application for the vacancy, it is desirable to mark the mandatory fields in the application. Failure to fill in the non-mandatory fields should not result in obstacles to move the person to the next stage.

Information received as a result of an undertaken test is personal data and they must be processed pursuant to the grounds and principles set by law.

3.2. Storage of Personal Data

In terms of storage of personal data, same as in other cases of personal data processing, it is necessary to comply with the principles established by the law. The employer must only **store the information, which is necessary for achieving the specific purpose of data processing.**

Example: if qualification and skills of the employees are assessed for the purpose of promotion and incentives, the work must be kept in a form that allows for identification of the employee, and until expiry of the term for appealing against the decision regarding promotions or incentives. After the term expires, if there is no need to keep the work, only the test results shall be kept.

Personal data must be stored for the term, which is required for the purpose of labor relations for which the data was gathered / processed, with exception of the cases when:

- Personal data of applicant/candidate is stored upon the consent of a data subject. For instance, individual agrees that his/her data are kept in reserve;
- The obligation of storing data for specific time is established by the law;
- Data are required for establishment of the fact of existence of labor relations.

Employer transfers the part of personal data processed for hiring into the employee's personal file, which is required for labor relations. Information that is no longer necessary to be stored, must be deleted or destroyed.

The employee must be informed about any data changes and/or corrections made into his/her personal file.

! Employee is responsible for accuracy, updating and security of personal data stored by him/her.

3.3. Employee's Consent to Process his/her Personal Data

In terms of labor relations, submission of documentation containing different types of personal data is established by legislation. In certain cases the basis for data processing is the consent of data subject (employee), which must be obtained in a form established by the law.

In accordance with the Law of Georgia on Personal Data Protection, consent constitutes the following: "**upon receipt of relevant information by the data subject, verbal or otherwise – via telecommunication or other appropriate mean - expressed voluntary consent on his/her data processing for definite purpose, which allows clear establishment of the will of data subject".**

In accordance with the law, inactivity cannot be viewed as consent, though provision of information containing personal data by applicant/candidate to the employer is considered as the consent of data subject.

Consent is given on:

- Data category;
- Purpose of data processing;
- Group of persons, to whom the data can be handed over;
- Conditions of data transfer to third person;

! In case of dispute, the burden of proof of existence of the consent is on the data controller (employer).

Consent may be issued only on processing of personal data of one's own or juvenile child/grantor.

! Employee's consent on personal data processing is not mandatory if there is other ground for data processing set forth in the Law of Georgia on Personal Data Protection, *for instance, legal requirement to provide employee's payroll information to tax authorities.*

Consent of data subject (employee) may be used as the grounds for data processing only in case when the employee has real chance to make independent decision regarding processing of his/her personal data.

The employee has the right to refuse further processing of data processed upon his/her consent. It must be considered that the refusal on consent does not have retroactive effect.

3.4. Purpose of Data Processing

Personal data must be processed for legal and clearly defined purpose. "Data processing" itself is not a purpose, and purpose cannot be of abstract or general nature. Purpose must be specific and easily understandable; *for instance, control over the employee to prevent disclosure of confidential information by such employee.*

Personal data must be used only for the purpose they were collected. If it is required to use personal data for other purpose, such purpose should not conflict with original purpose of processing and data subject must be duly informed.

Personal data must not be processed for the purpose, which is different from original purpose, if the employee has not given his/her consent on it or there is no other grounds for data processing for different purpose.

Example: organization decided to post the CVs and photos of its employees on its webpage. In such case it is necessary to inform the employees and obtain their consent (unless it is clearly stipulated in the contract or internal regulation of the organization), despite the fact that the organization is maintaining personal data on legal grounds.

Personal data should not be transferred to the third party without employee's consent, with exception of grounds determined by the law.

3.5. Processing of Special Category Data in Labor Relations

In accordance with the Law of Georgia on Personal Data Protection, special category data include information about person's race and ethnic origin, political views, religious or philosophic beliefs, membership of professional organizations/trade unions, health condition, sexual life or past conviction, also biometric data that allow person's identification by the above-mentioned features.

In accordance with the Law of Georgia on Personal Data Protection, processing of special category data is prohibited, with exception of cases mentioned in article 6 of the Law. One of the exceptions is necessity for data processing for the purpose of accomplishment of employment-related obligations or execution of any related rights by data controller. The above ground should not be interpreted broadly; special category data must be processed in proportion to legitimate purpose.

Example: employer asks employee to provide information about his/her blood typing, as some of them are hired on jobs with health damage risk. In such case, asking for blood typing information is legitimate. Though, imposition of the same requirement on other employees who deal with office tasks may be considered as asking for inadequate amount of information.

Law of Georgia on Public Service establishes the obligation of providing medical-drug certificate for persons starting their career at public service. For public institutions, this requirement serves as the basis for data processing. Similar requirement of private sector may be based on internal charter of the organization or other regulation.

It must also be taken into consideration that in the process of employment health-related information may be requested in order to establish one's fitness for performed job, for preventive medicine purposes, to establish one's capacity of work and for social security reasons.

Ability to process special category data for the purpose of fulfilling labor obligations does not mean that such basis can be used to justify intervention into privacy of an employee. *For instance, if a person has an appointment with a doctor during working hours, the employer has no right to request the diagnosis. This rule applies in cases when the employer has reasonable suspicion to believe that the person used working hours for some other purposes.*

In some cases the employer is authorized to process personal data if he/she has suspicion that the employee arrived at work under alcohol or drug intoxication. In such case it is necessary to keep balance between legitimate interest of the employer and employee's rights.

In case if the employee is asked to sign the consent on processing his/her special category data, the text of the consent must be made in a simple and plain language, and it should also indicate the form and duration of data processing.

The employer should not gather personal data related to political views, religious and philosophic beliefs, sexual life; such data can be gathered only under exceptional circumstances, in compliance with the rules established by Georgian legislation.

At the initial stage of the competition the employer must refrain from gathering special category data. Questions that related to special category data must be removed from the job application form. If necessary, such category data must be gathered from already selected candidates.

3.6. Job e-mail

In specific cases the employer has the right to control job email. In case of such control it is necessary to inform the employee.

Sometimes job email is used for **personal communications**. During communication control the employer must do its best to sort out personal and job-related emails and control only the job-related emails.

Best practice: employer must elaborate rules for use of corporate email, which will include information about the possibility of controlling email by the employer. If the employees use job email for personal communication, it is appropriate to place personal mail in a separate folder with appropriate indication (e. g. „private"). The employee must be informed about back-up copies and term of mail storage.

3.7. On-job Video Surveillance

Private and public institutions may carry out video control of the buildings for the purpose of monitoring, if it is required for protection of persons and property, protection of juveniles from detrimental influence and protection of secret information. It is allowed to monitor the external perimeter of the building and its entrance.

At job place, video surveillance system may be installed only under exceptional circumstances, if it is required for protection of individual's safety and property and if such aims cannot be accomplished otherwise. *For instance, video control at cashier's desk in the bank is required for protection of safety of the cashier and the bank, in order for security service to quickly respond to the incident.*

It must be considered that video surveillance does not automatically include audio monitoring (voice recording). Thus, during video surveillance it should not be possible to listen to employees' conversations, with exceptional cases (such as safety measures, etc.), upon which the employee should be informed.

All persons employed by private or public institutions must be informed in writing about on-job video surveillance and data subject's rights. Institutions must ensure the warning signs are visibly located in video control zones.

! Video surveillance is prohibited in locker rooms and hygiene closets.

3.8. Processing of Biometric Data

Organizations often process biometric data in the process when employees enter / move around the buildings, when they access electronic systems and technologies. In accordance with the Law of Georgia on Personal Data Protection, biometric data may be processed only for the purpose of protecting persons and property, also for preventing disclosure of secret information. Use of biometric data by private organizations is allowed for the purpose of carrying out its operation, if such purpose cannot be achieved otherwise or requires immeasurable effort. Biometric data must be processed on the basis of labor relations or special regulation, which shall include detailed conditions for processing of such data.

Example: use of fingerprints by the organization for determination of salaries and for timekeeping purposes is prohibited; in such case, salary and timekeeping can be controlled by other means, e.g. timekeeping system, registration log or card.

Prior to use of biometric data, private organization must provide Personal Data Protection Inspector with detailed information about processing of biometric data, including purpose of processing, protection safeguards and the information, which is provided to data subject.

4. Employee's Rights

In terms of personal data protection, the employee as a data subject has a number of rights, and realization of such rights guarantee personal data protection.

4.1. Right to Information/Access

The employee has the right to have information about processing of his/her personal data; in particular, which data are processed, for what purpose and means, and whether personal data are transferred to third parties, etc.

Employee must have access to his/her personal data, despite of the form of storage. He/she can obtain copy of a document and record containing his/her personal data. Employee's access to personal data must be unlimited and free of charge, with exceptions stipulated by law and cost of making copies.

When a person is hired through competition, the data controller is obliged to inform him/her about the conditions, results and score of the competition if so requested by the applicant. Besides, in case of the request, data controller is obliged to show any applicant (successful or unsuccessful) their written (electronic) work and provide information about assessment criteria.

When the employee announces the vacancy, together with the announcement the employee must also post his/her or hiring agency's (if such is involved) contact details, so that the applicants know who they provide information to and who is responsible for legal processing of their information.

4.2. Right to Ask for Correction, Update, Deletion, Destruction of Data

Employee has the right to ask for correction, update, addition, deletion, blocking or destruction of his/her data kept by the employer, if such data are incomplete, inaccurate, are not updated or if they were gathered and processed in violation of the law. Within 15 days from receipt of the data subject's request, the employer is obliged to carry out relevant action or inform the employee about the grounds for refusal.

4.3. Limitation of Employee's Rights

The above rights of the employee may be limited, if realization of such right endangers:

a) National security or defense interests of the country;

b) Public safety interests;

c) Uncovering of crimes, investigation and elimination;

d) Important financial or economic (including those related to monetary, budgetary, budget tax issues) interests;

e) Rights and freedoms of data subject and others.

Limitation can be applied only to the extent, which is necessary for achievement of the purpose of such limitation. Employer's decision about such limitation must be informed to the employee in a way the purpose of limitation of right is not damaged.

5. Employer Policy and Internal Regulation

In order for the employer to ensure protection of personal data in labor relations, it is desirable to have relevant internal policy and regulations, which would prescribe the issue of personal data protection and responsibility measures.

Any person, who has access to employees' personal data, is obliged to keep confidentiality of such information. There should be internal mechanisms for identification of violations of personal data protection law.

5.1. Ensuring Data Safety/Security

The Law of Georgia on Personal Data Protection obliges the employers to carry out necessary organizational-technical measures, which protect data from accidental and illegal destruction, amendment, disclosure, collection, any other form of illegal use and accidental or illegal loss. **Measures taken for protection of personal data must be adequate to risks related to data processing.**

Access to employees' personal data must be granted to those employees only, who have access to such data within the scope of their duty. In addition, they are responsible to act within the scope of their professional authority and to protect secrecy of the data, including after termination of their job authority.

When competition is announced on the vacancy and applications are received in an electronic format, safe/secure way for receiving the applications must be ensured. Applications received by mail or electronic applications must directly be handed over to the employee, which is individually involved in staff selection process.

In order to ensure security and proper functioning of automated systems, processed data should not be used to control behavior of the employee.

Example: if video surveillance is used in the organization for security reasons, it is prohibited to use video recordings to control employees' behavior. In exceptional circumstances, video recording must be used as evidence to resolve the dispute related to employee's behavior.

If data processor uses electronic program to control employees' personal data, access must be granted on the basis of proper authorization (e.g. access with password). Preference must be given to a so called "role based access control" system and access must be granted to limited number of persons, within the scope of job needs.

! If electronic database of employees' personal data is available to employer's branches, founders and/or partners, which are not subject to Georgian jurisdiction, it is necessary to comply with the rules of law regarding transfer of data to other state and international organization.

6. Employment via the Agency

On modern employment market staff is often selected via so called "employment agencies", which study the labor market, register those who want to find a job and select desirable candidates for employers.

For the purpose of the Law of Georgia on Personal Data Protection, in consideration of operational specifics, in some cases the employment agency acts as independent data controller, and in other cases it acts as data processor.

In case when employment agency collects personal data for its operational purposes (for instance, creation of the database of those wishing to get a job), it acts as data controller and is subject to the requirements set forth in the Law of Georgia on Personal Data Protection.

The approach is different when employment agency selects staff by the order of a specific employer. In such case the agency processes personal data for the purposes of the employer and acts as the data processor of the data controller (employer).

In accordance with the Law of Georgia on Personal Data Protection, data processor may process personal data on the basis of a legal act or a written contract concluded with the data controller. It is prohibited to conclude a contract on data processing with employment agency, if based on the operation or purposes of the agency there is risk of unreasonable use of such data. The employer must make sure that the agency takes organizational-technical measures that ensure protection of data from accidental and illegal destruction, amendment, disclosure, collection, any other form of illegal use. The employer is obliged to conduct monitoring/control over the data processing by the agency.

In case of termination of the contract between the employer and the agency, the data should immediately be transferred to the employer.