Georgian American University

Incident Identification and Response Policy

Contents

Article 1. General Information about the Data Controller

1. Georgian-American University LLC (hereinafter – the University) ensures the protection of fundamental human rights and freedoms, including privacy and personal data. The University places special emphasis on safeguarding the personal data of its employees and other individuals. Accordingly, it processes personal data in accordance with Georgian legislation, including the Law of Georgia on Personal Data Protection, other normative acts, and the internal policies adopted by the University in this area.

Article 2. Purpose of the Policy

1. The purpose of this policy is to establish a mechanism for the identification of incidents by the University, as a data controller, to ensure timely response and to fulfill the obligations stipulated by the Law of Georgia on Personal Data Protection.
2. The University acts in accordance with the Law of Georgia on Personal Data Protection and other normative acts when responding to incidents.

Article 3. Definitions of Terms

The following terms used in this policy shall have the meanings indicated below:

a) Personal Data (hereinafter – Data):
Any information relating to an identified or identifiable natural person. A natural person is considered identifiable when they can be identified, directly or indirectly, in particular by reference to a name, surname, identification number, geolocation data, electronic communication identifiers, or one or more factors specific to the physical, physiological, mental, psychological, genetic, economic, cultural, or social identity of that person.

b) Special Category Data:
Data that pertains to a person's racial or ethnic origin, political opinions, religious, philosophical or other beliefs, trade union membership, health, sexual life, legal status in a criminal proceeding (accused, convicted, acquitted, or victim), criminal conviction, sentencing, diversion, status as a victim of trafficking or a crime under the Law of Georgia on Elimination of Violence Against Women and/or Domestic Violence, victim protection and

assistance, imprisonment and enforcement of sentences, as well as biometric and genetic data processed for the purpose of uniquely identifying a natural person.

c) Health Data:
Information about a data subject's physical or mental health, including data revealing details about medical treatment received, if such information provides insights into the subject's physical or mental condition.

d) Data Controller:
A natural person, legal entity, or public institution that, independently or jointly with others, determines the purposes and means of data processing, and performs the processing either directly or through an authorized data processor.

e) Data Processing:
Any operation performed on data, including collection, acquisition, access, photographing, video or audio monitoring, organization, categorization, correlation, storage, modification, retrieval, request, use, blocking, deletion, or destruction, as well as disclosure through transmission, publication, dissemination, or otherwise making the data accessible.

f) Data Subject:
Any natural person whose data is being processed.

Article 4. Definition and Types of Incidents

1. An incident is a breach of personal data security (including organizational, physical, or technical), which results in the unauthorized or accidental damage, loss, unauthorized disclosure, destruction, alteration, access, collection/acquisition, or any other form of unauthorized processing of personal data.
2. Types of incidents include:
    - a) Breach of confidentiality – unauthorized disclosure of or access to personal data;
    - b) Breach of integrity – unauthorized alteration, unlawful or accidental damage or loss of personal data;
    - c) Breach of availability – loss or restriction of access to personal data, destruction or deletion of data.

Article 5. Incident Identification Procedure

1. If a person involved in the processing of personal data at the university (employee or authorized processor, if applicable) discovers any type of personal data security breach, including unauthorized or accidental damage, loss, disclosure, destruction, alteration, access, collection/acquisition, or other unauthorized processing, they must immediately, but no later than within 24 hours, notify the University's Data Protection Officer (DPO) using any possible communication means (phone call, email, text message, or other available method).
2. Failure to fulfill the obligation under paragraph 1 may result in the initiation of disciplinary proceedings for the responsible staff member (or other authorized person, if applicable), in accordance with their employment contract, internal regulations, or other internal university policies. In case of confirmed misconduct, disciplinary or legal actions may follow.
3. The notification referred to in paragraph 1 must include the following information:
    - Date of the incident;
    - Type of incident (short description);
    - Description/content of the breach;
    - Description of the data involved in the incident;
    - Consequences of the incident;
    - Estimated number of affected individuals;
    - Estimated damage caused by the incident, its scale.
4. Based on the notification, the University Data Protection Officer shall immediately begin an investigation into the incident and related factual circumstances, and evaluate the outcome, the degree of actual or potential harm, and the level of risk.
5. An incident shall be considered as causing significant harm to fundamental rights and freedoms if it results or is likely to result in any of the following:
    - a) Discrimination against the data subject, identity theft or fraud, financial loss, reputational damage, breach of confidentiality of professional or sensitive personal data, or other significant social and/or economic harm;
    - b) Obstruction of the data subject's ability to exercise their legal rights, including delays in exercising such rights within legal timeframes;
    - c) Deletion/destruction of personal data that cannot be restored, or whose restoration would require disproportionately large time and effort, except where such deletion/destruction (excluding special category data) does not cause significant harm as defined in subparagraphs "a" through "e";
    - d) Unlawful disclosure of special category data;
    - e) Unlawful processing of personal data of minors, persons with disabilities, or others in need of special social or legal protection.

6. The likelihood of significant harm or risk to human rights and freedoms resulting from the incident is categorized as follows:
    - a) Low – if it is unlikely that the incident will cause significant harm or pose a significant threat;
    - b) Medium – if the likelihood of harm/threat and non-harm/non-threat is roughly equal;
    - c) High – if the incident is likely to cause significant harm or pose a serious threat to rights and freedoms.

Article 6. Circumstances to Consider When Assessing the Severity of Significant Threats Arising or Expected from an Incident

For the purpose of determining the severity of a significant threat to human rights and freedoms resulting from an incident, the University takes into account and evaluates the following circumstances:

a) The type of incident that has occurred (i.e., breach of the confidentiality, integrity, or availability of personal data);

b) The category of personal data affected by the incident;

c) Whether the incident involves the personal data of a minor, a person with disabilities, or another individual requiring special social or legal protection;

d) The degree to which the data subject can be identified by third parties as a result of the incident;

e) The special nature of the data controller's (responsible party's) activity, which may involve elevated risk;

f) The scale of the incident, in terms of the number and/or volume of data subjects and/or personal data affected;

g) Any other circumstances that may have a substantial impact on the likelihood and severity of a significant threat to human rights and freedoms resulting from the incident.

Article 7. Incident Response Procedure

1. The University, with the active involvement of the Data Protection Officer (DPO), ensures the registration of incidents, their outcomes, and the measures taken, in the form specified in Annex No.1 of this Policy (Register of Incidents Containing a Significant Threat to Fundamental Human Rights and Freedoms).
2. An incident is considered discovered, and the University is considered informed about the incident, from the moment it becomes aware of it.
3. From the moment of discovery or notification of the incident, the University—without undue delay and with the active participation of the Data Protection Officer and, if necessary, the relevant structural units, including the IT Department—takes all appropriate technical and organizational measures to accurately identify the incident, detect the harmful consequences, and ensure effective mitigation.
4. The University's Data Protection Officer ensures that the incident is reported in writing or electronically to the Personal Data Protection Service within no later than 72 hours of discovery, if the incident is likely to cause, or poses, a medium or high probability of significant harm to fundamental human rights and freedoms.
5. The notification to the Personal Data Protection Service must include the following information:
    - Circumstances, type, and time of the incident;
    - Estimated categories and volume of data that were unlawfully disclosed, damaged, deleted, destroyed, obtained, lost, or modified, and the categories and number of data subjects potentially affected;
    - The anticipated consequences of the incident and the measures taken or planned by the University to reduce or eliminate the impact;
    - Whether the University intends to notify the data subject(s) and within what timeframe;
    - Contact details of the Data Protection Officer or other relevant contact person.
6. In addition to the information listed in point 5, the University must also submit information as defined under Article 10 of Order No. 19 (dated 28 February 2024) issued by the Head of the Personal Data Protection Service on the "Approval of Criteria for Defining Incidents Involving a Significant Threat to Fundamental Rights and Freedoms and the Procedure for Notifying the Personal Data Protection Service."
7. If a full assessment of the incident cannot be completed within 72 hours, but there is reasonable suspicion that it poses a medium or high risk of significant harm, the University must not delay notification. In such cases, if the University is unable to provide all required information due to objective reasons, it will submit the information incrementally within a reasonable timeframe, without undue delay.

8. If it is unlikely that the incident will cause or pose significant harm to fundamental rights and freedoms, the University is not obligated to notify the Personal Data Protection Service.

Article 8. Obligation to Inform the Data Subject About an Incident

1. If an incident is highly likely to cause significant harm or pose a significant threat to fundamental human rights and freedoms, the University is obliged to inform the data subject of the incident at the first opportunity, without undue delay, and provide the following information in clear and understandable language:
   a) A general description of the incident and its related circumstances;
   b) The potential or actual harm caused by the incident, and the measures taken or planned to mitigate or eliminate the damage;
   c) Contact details of the Data Protection Officer or another designated contact person.
2. If notifying the data subject requires disproportionate effort or cost, the University may publicly disseminate the information in a manner that ensures the data subject can reasonably access it.
3. The obligations described in Paragraphs 1 and 2 do not arise if:
   a) Notifying the data subject would threaten state secrecy, national security, information security, cybersecurity, or defense interests, public safety, crime prevention, operational-search activities, criminal investigation, prosecution, justice, imprisonment or enforcement of non-custodial sentences and probation, or important financial, economic, public health, or social welfare interests of the country;
   b) The University has implemented appropriate security measures that have prevented any significant threat to fundamental human rights and freedoms.

Article 9. Measures for Incident Prevention

1. The University has implemented all necessary organizational and technical measures to prevent incidents to the greatest extent possible, ensure their timely detection, and effectively eliminate the consequences.
2. The University regularly educates its employees about the nature of personal data and the importance of its protection, by organizing informative meetings, training sessions, and practical courses focused on the identification and effective response to incidents.
3. The University ensures that employees involved in data processing, and where applicable, authorized processors, are bound by legal mechanisms and obligations to promptly identify and respond to incidents in compliance with legal requirements.

Article 10. Mechanisms for Protecting the Rights of the Data Subject

1. The University ensures the protection of the rights of the data subject as defined under Chapter III of the Law of Georgia on Personal Data Protection.
2. For any issue related to data processing, the data subject is entitled to contact the Head of the University's Human Resources Department and/or the Data Protection Officer.
3. In case of a dispute related to personal data protection, the data subject has the right to appeal to the Personal Data Protection Service and/or the court in accordance with the law