Утверждено Ученым советом ТГУ на 2025 год
Постановлением № 07 от 2 мая

Политика обработки персональных данных

1. Общая информация о документе

Политика обработки персональных данных (далее – Политика) направлена на обеспечение прозрачности обработки персональных данных юридическим лицом «Тбилисский гуманитарный университет» (далее – Университет). Политика позволяет любому лицу, в том числе субъекту персональных данных и/или потенциальному субъекту персональных данных, получить информацию об обработке персональных данных учреждением на простом и понятном языке.

Персональные данные (далее – данные) – это любая информация, относящаяся к идентифицированному или идентифицируемому физическому лицу. Физическое лицо считается идентифицируемым, если его можно идентифицировать прямо или косвенно, в том числе по имени, фамилии, идентификационному номеру, данным геолокации, идентификатору электронной связи, физическим, физиологическим, психическим, психологическим, генетическим, экономическим, культурным или социальным характеристикам.

Обработка персональных данных осуществляется в соответствии с законодательством Грузии, в частности, Законом Грузии «О защите персональных данных» и другими нормативными актами.

Права субъекта данных защищены как законодательством Грузии, так и в соответствии с Европейским регламентом по защите данных (GDPR).

Обработка персональных данных осуществляется в соответствии с законодательством Грузии и международным законодательством, в частности, следующими принципами, предусмотренными GDPR:

- Принцип справедливости;
- Прозрачность;
- Принцип ограничения цели;
- Принцип минимизации данных;
- Принцип минимизации терминов;
- Принцип точности данных;
- Принцип безопасности.

Политика обеспечивает соблюдение подпункта «а» пункта первого статьи 4 Закона Грузии «О защите персональных данных», который согласно ему, обработка данных должна осуществляться законно, справедливо, прозрачно для субъекта данных и без ущемления его достоинства.

Термины, используемые в Политике, имеют значения, определенные в Законе Грузии «О защите персональных данных».

Политика доступна на веб-сайте университета, и все субъекты данных имеют возможность ознакомиться с ней.

2. Общая информация о деятельности ООО «Премиум Сэйфти»

ООО «Премиум Сэйфти» — консалтинговая компания, обеспечивающая соблюдение законодательства компаниями-партнерами в различных областях. Одним из направлений

деятельности компании является предоставление услуг специалиста по работе с персональными данными, назначение специалиста, ведение полного документооборота и приведение деятельности компании-клиента в соответствие с законодательством.

3. Общие сведения о лице, ответственном за обработку данных

ООО «Тбилисский гуманитарный университет» – высшее учебное заведение, осуществляющее обработку данных студентов, сотрудников и иных третьих лиц, в том числе несовершеннолетних, в целях осуществления своих функций. Обрабатываемые данные о субъектах включают персональные данные студентов и сотрудников, информацию об успеваемости и деятельности студента в период обучения в университете.

Защита персональных данных является правом всех членов общества, поэтому обработка данных представляет собой четко регламентированный процесс, и университет обеспечивает защиту персональных данных всех членов, для чего разработал политику обработки персональных данных и назначил ответственного за защиту персональных данных.

4. Общие сведения о лице, уполномоченном на обработку данных

4.1. Университет имеет уполномоченных сотрудников по обработке данных, которые обрабатывают данные только в законных целях Университета, регламентируются вопросы защиты персональных данных, а уполномоченное лицо (лица) обязуются обеспечивать конфиденциальность обрабатываемых ими в рамках оказания услуг данных.

4.3. Университет осуществляет контроль за техническими и организационными мероприятиями, а также за обработкой данных уполномоченными лицами при исполнении ими своих функций и обязанностей.

4.4. Университет обязан по требованию субъекта (субъектов) данных предоставить информацию об уполномоченном лице (лицах) в порядке, установленном Законом Грузии «О защите персональных данных».

5. Правила обработки персональных данных ООО «Тбилисский гуманитарный университет»

5.1 Преамбула

Правила обработки персональных данных в Университете разработаны на основании Закона Грузии «О защите персональных данных» и других нормативных актов. Правила обработки персональных данных в Университете применяются учреждением при обработке данных субъектов и распространяются на любые формы обработки данных учреждением.

5.2. Лицо, ответственное за обработку данных:

ООО «Тбилисский гуманитарный учебный университет» - зарегистрировано в соответствии с законодательством Грузии как юридическое лицо публичного права.

Идентификационный код: 2060046045

Адрес: Тбилиси, Исанский район, проспект Бери Габриэля Салоси, 31.

Номер телефона:

Электронная почта: thu-posta@thu.edu.ge

5.3 Сотрудник по защите персональных данных:

ООО «Премиум Сэйфт»

Идентификационный код: 405656320

Адрес: Тбилиси, район Ваке, улица Кипшидзе N2, дом 2б, 73

Номер телефона: (+995) 577 17 64 61

Электронная почта: zura.gujabidze@geosafety.ge

5.4 «Политика обработки персональных данных»

Статья 1. Общие положения

1. Настоящее правило регулирует вопросы, связанные с обработкой персональных данных Университетом.

2. Настоящий документ распространяется на любого лица, работающего в Университете и действующего от имени Университета, а также на стажеров (при наличии) и является обязательным для исполнения.

3. Настоящее правило применяется в соответствии с Законом Грузии «О защите персональных данных».

Статья 2. Определение терминов

1. Для целей настоящего правила термины, используемые в настоящем правиле, имеют значения, предусмотренные Законом Грузии «О защите персональных данных»:

а) Персональные данные (далее – данные) – любая информация, относящаяся к идентифицированному или идентифицируемому физическому лицу. Физическое лицо считается идентифицируемым, если оно может быть идентифицировано прямо или косвенно, в том числе по имени, фамилии, идентификационному номеру, данным геолокации, данным идентификации электронной связи, физическим, физиологическим, психическим, психологическим, генетическим, экономическим, культурным или социальным характеристикам;

б) данные специальной категории – данные, касающиеся расового или этнического происхождения физического лица, его политических взглядов, религиозных, философских или иных убеждений, членства в профсоюзе, состояния здоровья, половой жизни, статуса обвиняемого, осужденного, оправданного или потерпевшего в уголовном процессе, осуждения, вынесения приговора, признания жертвой торговли людьми или преступления в соответствии с Законом Грузии «О предотвращении насилия в отношении женщин или (и) насилия в семье, защите и помощи жертвам насилия», лишения свободы и исполнения наказания, а также биометрические и генетические данные, обработанные в целях однозначной идентификации физического лица;

в) данные, связанные со здоровьем, — информация о физическом или психическом здоровье субъекта данных, а также информация об оказании ему медицинских услуг, если она дает информацию о физическом или психическом здоровье субъекта данных;

г) Биометрические данные - данные, относящиеся к физическим, физиологическим или поведенческим характеристикам субъекта данных (такие как, например, изображение лица, характеристики голоса или дактилоскопические данные), обрабатываемые с использованием технических средств, что позволяет однозначно идентифицировать его или подтвердить его личность;

е) Обработка данных – любое действие, совершаемое над данными, включая их сбор, извлечение, доступ к ним, их фотографирование, Видеонаблюдение и/или аудионаблюдение, организация, группировка, объединение, хранение, изменение, восстановление, извлечение, использование, блокирование, удаление или уничтожение, а также раскрытие данных путем передачи, публикации, распространения или предоставления иным способом;

ж) Автоматизированная обработка данных - обработка данных с использованием информационных технологий;

з) Неавтоматизированная обработка данных – обработка данных без использования информационных технологий;

и) Полуавтоматическая обработка данных — обработка данных с использованием комбинации автоматических и неавтоматических средств;

j) Файловая система – структурированный набор данных, в котором они организованы и доступны в соответствии с определенными критериями;

л) Субъект данных — любое физическое лицо, в отношении которого обрабатываются данные;

н) Согласие субъекта персональных данных - свободно и ясно выраженная воля субъекта персональных данных после получения соответствующей информации на обработку данных о нем в определенном целях путем совершения им активных действий в письменной (в том числе в электронной форме) или устной форме;
о) Письменное согласие субъекта данных - согласие, которое субъект данных подписал или иным образом выразил в письменной форме (в том числе в электронной форме) после получения соответствующей информации на обработку касающихся его данных для определенной цели;
н) Лицо, ответственное за обработку, - физическое лицо, юридическое лицо или государственное учреждение, которые самостоятельно или совместно с другими определяют цели и средства обработки данных и осуществляют обработку данных непосредственно или через лицо, уполномоченное на ее обработку;
р) Совместные контролеры – два или более контролеров, которые совместно определяют цели и средства обработки данных;
(р) Обработчик данных – физическое лицо, юридическое лицо или государственное учреждение, которые обрабатывают данные от имени или по поручению контролера данных. Физическое лицо, состоящее в трудовых отношениях с контролером данных, не считается обработчиком данных;
т) Получатель данных – физическое лицо, юридическое лицо или государственное учреждение, которым были переданы данные, за исключением Службы по защите персональных данных;
(s) Инцидент — нарушение безопасности данных, которое приводит к незаконному или случайному повреждению, потере или несанкционированному раскрытию, уничтожению, изменению, доступу, сбору/извлечению или другой несанкционированной обработке данных.
2. Иные термины, содержащиеся в настоящих Правилах, если не указано иное, толкуются в соответствии с Законом Грузии «О защите персональных данных».

Статья 3. Цели обработки данных
Целями обработки персональных данных Университетом являются:
а) осуществление образовательной деятельности;
б) осуществление служебной деятельности;
в) обеспечение бесперебойности образовательного процесса;
г) обеспечение бесперебойности рабочего процесса;
д) Регистрация студентов;
е) Ведение личных дел студентов и сотрудников;
ж) Обеспечение регистрации и оценки студентов;
з) Реализация права на образование для обучающихся с особыми образовательными потребностями;
i) Совершенствование баз данных в целях разработки электронной системы оценки;
к) Организация и контроль документооборота;
л) выдача документа, подтверждающего высшее образование;
н) Обеспечение вовлечения студентов и сотрудников в различные мероприятия;
n) Предоставление информации, запрашиваемой ЮЛПП - Информационной системой управления образованием, загрузка данных в ее базу данных;
о) обеспечение физической безопасности имущества учреждения, сохранности его активов, а также сотрудников и/или студентов;
о) осуществление иных полномочий, возложенных законом.
Статья 4. Основы обработки данных
1. Обработка персональных данных осуществляется по следующим основаниям:

а) субъект данных дал согласие на обработку данных, касающихся его или ее, для одной или нескольких конкретных целей;
б) обработка данных необходима для исполнения обязательства по договору, заключенному с субъектом данных, или для заключения договора по требованию субъекта данных;
в) Обработка данных необходима для выполнения учреждением своих обязательств в соответствии с законодательством;
г) Обработка данных предусмотрена законом;
д) в соответствии с законом данные являются общедоступными или субъект данных сделал их общедоступными;
е) обработка данных необходима для защиты жизненно важных интересов субъекта данных или иного лица;
g) обработка данных необходима для защиты важных законных интересов лица, ответственного за обработку, или третьего лица, за исключением случаев, когда преобладающий интерес заключается в защите прав субъекта данных (в том числе несовершеннолетнего);
з) Обработка данных необходима для обработки заявления субъекта данных (для предоставления ему услуги).
2. Учреждение осуществляет обработку специальных категорий данных только в случае, если:
а) Данные обрабатываются в целях реализации права на образование лиц с особыми образовательными потребностями;
б) Обработка данных о судимостях за преступления против половой свободы и неприкосновенности, а также о состоянии здоровья необходима исходя из характера трудовых обязательств и отношений. В том числе для принятия решения о трудоустройстве. Согласно части 2 статьи 32 Закона Грузии «О высшем образовании»: Лицо, осужденное за совершение преступления против половой свободы и неприкосновенности, предусмотренного Законом Грузии «О борьбе с преступлениями против половой свободы и неприкосновенности», и (или) лицо, лишенное судом права на работу в образовательном учреждении на основании того же закона, не может быть трудоустроено в высшем образовательном учреждении.
3. В случае, если учреждение обрабатывает данные с согласия субъекта данных, согласие считается действительным только в том случае, если оно дано после получения соответствующей информации, добровольно, для достижения конкретной и конкретной цели обработки данных. Согласие дается добровольно и при активном участии субъекта данных.

Статья 5. Субъекты данных
Университет обрабатывает персональные данные следующих лиц:
а) действующих и бывших работников, в том числе лиц, работающих по трудовому договору;
б) Кандидаты, участвующие в конкурсе, объявленном на замещение вакантных должностей;
в) студенты;
г) Несовершеннолетние [1];
[1] В исключительных случаях . В частности, когда студент поступает на первый курс и ему ещё не исполнилось 18 лет. В таком случае , как и все студенты , несовершеннолетний должен предоставить все необходимые документы вместе с законным представителем .
д) подрядчики/уполномоченные представители подрядчиков, состоящих в договорных отношениях с организацией;
е) Другие лица, находящиеся в зоне видеонаблюдения.
Статья 6. Права субъекта данных
1. Субъект данных имеет право:
а) получать информацию об обработке своих данных;
б) получать информацию о сообработчике данных и/или уполномоченном лице;

в) получать информацию о целях, основаниях и категориях обработки данных;
г) получать информацию о личности или категории получателей данных, которым данные были переданы или будут переданы в будущем;
д) получать информацию о сроке хранения данных или, если конкретный срок не может быть определен, о критериях определения срока;
f) получить любую доступную информацию об источнике сбора данных, если данные не собираются непосредственно от субъекта данных;
ж) запрашивать доступ к данным и получать копию;
h) Требовать немедленного исправления, обновления, переноса или удаления неверных/неточных данных, обработанных о нем/ней или в целях обработки данных.Учет, восполнение неполных данных, в том числе путем представления дополнительных сведений/документов;
i) требовать прекращения обработки данных, удаления данных или уничтожения данных по запросу на согласие;
j) Запрос на блокировку данных.
2. Для осуществления прав, предусмотренных частью первой настоящей статьи, субъект персональных данных должен обратиться к лицу, уполномоченному на обработку персональных данных, или к лицу, ответственному за обработку, если персональные данные хранятся у него.
3. Субъект данных информируется в соответствии с политикой о том, кто несет ответственность за хранение данных и реагирование на запросы, сделанные в рамках вышеуказанных прав субъекта данных, в рамках отношений между университетом и конкретной организацией.
4. В случае поступления запроса от субъекта персональных данных Университет обязан предоставить субъекту персональных данных соответствующую информацию не позднее 10 (десяти) рабочих дней со дня получения уведомления о запросе. Указанный срок может быть продлен не более чем на 10 рабочих дней в исключительных случаях при наличии обоснования, о чем субъект персональных данных должен быть незамедлительно уведомлен.
5. Субъект данных имеет право отозвать своё согласие в любое время без объяснения причин или обоснования. Отзыв согласия может быть осуществлён в том же порядке, в котором оно было предоставлено.
6. Права субъекта данных могут быть ограничены в случаях и порядке, предусмотренных Законом Грузии «О защите персональных данных».
7. В случае, если действия, необходимые для реализации прав субъекта персональных данных, относятся к компетенции иных органов, участвующих в процессе обработки персональных данных, например, Службы по защите персональных данных, учреждение вправе разъяснить это субъекту персональных данных в письменной форме.
8. Субъект персональных данных пользуется всеми иными правами субъекта, предусмотренными Законом о защите персональных данных.
9. Субъект персональных данных имеет право обратиться по любому вопросу, связанному с обработкой персональных данных, к ректору Университета и/или должностному лицу по защите персональных данных.
10. В случае возникновения спора по вопросам, связанным с защитой персональных данных, субъект персональных данных вправе обратиться в Службу по защите персональных данных и (или) в суд в порядке, установленном законодательством.
Статья 7. Категория данных
В зависимости от характера отношений с субъектом данных и цели обработки данных при необходимости могут обрабатываться следующие персональные данные:
а) Идентификационные данные - имя, фамилия, личный номер, копия удостоверения личности, фотография, дата рождения, пол;
б) Контактные данные - юридический и фактический адреса, телефон, электронная почта;

в) Данные специальной категории:
в.а) Сведения о судимостях за преступления против половой свободы и половой неприкосновенности научно-педагогических и административных работников, обработка которых необходима в силу характера трудовых обязательств и отношений, в том числе для принятия решений о приеме на работу;
в.б) больничный лист работника;
г) Заверенные копии дипломов;
д) статус занятости;
е) иная информация, предусмотренная соответствующей службой, а также нормативными актами университета.
ж) Опыт работы - должность, наименование должности, заработная плата, квалификация, вознаграждение;
з) заявление и (или) документ, подтверждающие согласие работника на установление трудовых отношений;
i) Копия документа, удостоверяющего личность/паспорта;
к) Копия документа об образовании или соответствующей квалификации, сертификата, подтверждающего педагогический стаж.
k) Свидетельство об окончании школы;
н) Автобиография - резюме (CV);
о) 1 фотография в цифровом формате;
n) Официальные реквизиты действующего банковского счета;
п) документ, подтверждающий выход из пенсионной системы в рамках накопительной пенсионной реформы, при наличии;
р) В случае применения льготы по подоходному налогу – документ, подтверждающий это – справка из Налоговой службы; с) Учебные программы в печатном и электронном виде
т) Документ, подтверждающий владение иностранным языком;
т) Видеоизображения других лиц, находящихся в зоне видеонаблюдения;
(u) Военное свидетельство (в случае, если военнослужащий – мужчина);
е) военный билет (для студентов мужского пола);
v) В случае мобильности – справка/табель успеваемости из предыдущей школы;
ж) Информация об успеваемости студента;
(k) Информация о предыдущем университете (университетах), в котором(ых) учился студент;
(з) Правовые акты, определяющие статус студента;
в) Идентификационные данные умерших студентов - для целей регистрации умершего студента или прекращения статуса студента в базе данных Министерства образования, науки и молодежи.

Статья 8. Источники сбора данных
Источниками персональных данных, получаемых Университетом, являются:
а) предоставление данных на основе явного, активно выраженного согласия субъекта данных;
б) данные, полученные с помощью видеонаблюдения;
в) Данные, полученные с электронного портала (thu.edu.ge), в котором субъект заполняет свое имя, фамилию, номер телефона и адрес электронной почты;
г) Получение данных из информационной системы управления высшим образованием;
д) Получение информации из любого законного источника в целях, указанных в настоящем Правиле и/или законе.

Статья 9. Безопасность данных и обязанности сотрудников

1. Университет обеспечивает безопасность данных путем принятия соответствующих организационных и технических мер для их защиты от случайного или незаконного уничтожения, изменения, раскрытия, извлечения, любой другой формы незаконного использования, а также случайной или незаконной утраты.

2. Университет обязан предоставить субъекту данных подробную информацию о том, какие данные он собирает, как он их использует, кому он их передает и как он защищает безопасность данных.

3. Любое лицо, работающее в Университете и участвующее в обработке данных или имеющее доступ к данным, обязано:

а) не превышать объем предоставленных ему полномочий;

б) обеспечивать сохранение тайны и конфиденциальности данных, в том числе после прекращения полномочий должностных лиц;

в) не использовать данные в личных, неслужебных целях;

г) не предоставлять данные неуполномоченным лицам, в том числе путем оставления данных без присмотра и/или просмотра их в присутствии неуполномоченных лиц.

4. Нарушение правил, установленных настоящим документом, является нарушением правил внутреннего трудового распорядка Университета и может повлечь за собой применение соответствующих дисциплинарных взысканий.

5. Доступ к данным имеют только те сотрудники, которым они необходимы для выполнения своих функций и обязанностей.

6. Доступ к электронным системам, используемым Университетом, возможен только с использованием индивидуального имени пользователя и пароля, содержащего сложную комбинацию, обновляемую один раз в 3 месяца. Разглашение/передача имени пользователя и пароля кому-либо запрещается.

7. Действия, совершаемые с данными в электронной форме, должны регистрироваться/регистрироваться в соответствующих электронных журналах. При обработке данных в неэлектронной форме ответственное лицо (лица), работающие в учреждении, должны обеспечить регистрацию всех действий (включая информацию об инцидентах), связанных с раскрытием и/или изменением данных.

8. Данные хранятся на защищённом сервере университета, расположенном в Грузии, а именно в Тбилиси, по адресу: проспект Бери Габриэля Салоси, д. 31. Он запирается механическим ключом. IT-менеджер имеет полный доступ к серверу.

9. Университет выделил отдельное, специально защищённое помещение для хранения данных в архивном виде. Доступ в это помещение осуществляется по специальному разрешению и регистрации.

10. Данные специальной категории хранятся в кабинете Службы управления персоналом и делопроизводства и доступны только уполномоченным лицам. Обеспечена система безопасности и учёта доступа.

11. Университет разрабатывает документ об оценке воздействия на защиту данных, который должен включать: описание категорий данных, целей, пропорциональности, процесса и оснований их обработки; оценку возможных угроз основным правам и свободам личности и описание организационных и технических мер, принимаемых для защиты безопасности данных.

Статья 10. Сроки хранения данных

1. Университет хранит только те данные, которые необходимы для достижения конкретной, законной цели обработки данных.

2. Специальные категории данных должны храниться как автоматизированными, так и неавтоматизированными средствами в течение периода, необходимого для достижения законной цели, для которой контролер и субъекты данных несут ответственность за обработку персональных данных.

3. Хранение персональных данных осуществляется в соответствии со сроками, установленными законодательством. При необходимости определения сроков и правил хранения персональных данных Университет учитывает принципы обработки персональных данных.

4. Для хранения данных на физических носителях в Университете устанавливаются следующие сроки : [2]

[2] Помимо перечисленных в вышеуказанной статье, при определении сроков университет руководствуется «Приказом министра юстиции Грузии «Об утверждении перечня типовых административных документов, создаваемых в процессе деятельности учреждений (с указанием сроков их хранения)» от 31 марта 2010 года, г. Тбилиси, № 72.

а) Личные дела сотрудников хранятся в течение 75 лет;

б) Личные дела студентов хранятся в течение 75 лет;

в) Листы учета рабочего времени хранятся в течение 1 года.

г) Информация о кандидатах, участвующих в конкурсе, объявленном на замещение вакантных должностей, хранится в течение 1 года.

д) протокол заседания коллегиального органа - сроком на 5 лет.

5. Документация на бумажных носителях (текущие документы, активные личные дела) хранится в Службе управления персоналом. Доступ к документам и/или хранящейся в них информации возможен только после получения указанной документации от руководителя Службы управления персоналом и ее соответствующей регистрации.

6. Документация на бумажных носителях (личные дела, протоколы заседаний коллегиальных органов), не находящиеся в оперативном использовании, сдаётся в архив и хранится в специально отведённом помещении. Помещение запирается на ключ, который хранится у начальника службы управления персоналом. Доступ к архивным документам возможен с разрешения директора при наличии соответствующего письменного основания.

7. По истечении срока хранения документы на бумажных носителях подлежат уничтожению, о чем составляется соответствующий акт.

Статья 11. Доступ к данным

1. Сотрудники имеют доступ к данным только в том объеме и в той мере, которые необходимы для выполнения ими своих должностных обязанностей. В случае, если сотрудник находится в отпуске или по иной причине, а его должностные обязанности исполняет другое лицо, доступ последнего к информации определяется возложенными на него должностными обязанностями.

2. (QMS.EQE.GE) имеет доступ к:

а) Начальник службы управления персоналом

5. Служба управления персоналом имеет право доступа к личным делам (материальным документам) работников и (или) к материалам дела, содержащимся в личном деле.

6. Секретариаты соответствующих факультетов имеют право доступа к личным делам (материальным документам) студентов и/или материалам дела, содержащимся в личных делах.

7. О системе документооборота и содержащейся в ней информации:

а) Ректор и начальник Службы управления персоналом имеют полный доступ для обеспечения распределения входящей корреспонденции и надлежащего реагирования;

б) имеют ограниченный доступ — другим сотрудникам разрешено просматривать направленную им корреспонденцию и готовить соответствующие ответы.

Статья 12. Передача/раскрытие данных

1. Обрабатываемые Университетом данные могут быть переданы следующим третьим лицам в порядке и объеме, установленных законодательством, при наличии законных оснований:

а) правоохранительные органы;

б) суд;

в) Служба по защите персональных данных;

г) иные органы, предусмотренные законом.

2. Данные также могут передаваться:

а) Министерство образования, науки и молодежи;

б) Министерство юстиции;

в) Министерство обороны;

г) правоохранительные органы;

д) органы государственной власти и (или) органы местного самоуправления в случаях, предусмотренных законом;

f) международная организация, когда это необходимо для академических, административных целей в интересах студентов и сотрудников;

ж) Национальный центр развития качества образования, в системе Министерства образования, науки и молодежи Грузии;

h) Информационная система управления образованием;

i) Налоговая служба;

к) иные лица, предусмотренные законом.

3. В случаях, предусмотренных пунктами 1 и 2 настоящей статьи, при раскрытии информации университет обязан фиксировать, какие данные были раскрыты, кому, когда и на каком правовом основании. Указанная информация хранится вместе с данными о субъекте в течение срока их хранения.

Статья 13. Видеонаблюдение

1. Университет использует систему видеонаблюдения для выполнения своих обязанностей, предусмотренных законодательством, – обеспечения безопасности граждан и имущества, а также защиты несовершеннолетних от вредного воздействия. Кроме того, Университет вправе осуществлять видеонаблюдение во время проведения экзаменов.

2. Для информирования субъектов данных об обработке данных в здании на видных местах размещаются соответствующие предупреждающие знаки.

3. Университет обеспечивает надлежащее информирование работников, рабочее место которых попадает в поле зрения системы видеонаблюдения.

4. Система видеонаблюдения и записи защищены от несанкционированного доступа и использования. Доступ к ней осуществляется по имени пользователя и паролю.

5. Система видеонаблюдения защищена шифрованием и оснащена соответствующим механизмом самоуничтожения. Определен круг лиц, имеющих доступ к данным, полученным в результате видеонаблюдения, который представлен:

а) ИТ-менеджер — полный доступ.

6. Срок хранения данных, полученных посредством видеонаблюдения, составляет 30 календарных дней, после чего данные автоматически уничтожаются системой.

7. Зона видеонаблюдения включает в себя:

а) общая территория учреждения;

б) коридоры;

в) «Фойе»

г) Внешний периметр учреждения, который включает в себя - внешнее пространство учреждения, вход.
8. Видеонаблюдение не осуществляется в раздевалках, помещениях, предназначенных для соблюдения гигиены, а также в пространстве, где субъект имеет разумные ожидания конфиденциальности и/или осуществление видеонаблюдения противоречит общепринятым нормам морали.

Статья 14. Контроль доступа к системе видеонаблюдения
В системе видеонаблюдения университета определены следующие виды доступа:
а) Мониторинг камер видеонаблюдения в реальном (онлайн) режиме — пользователь с таким доступом может только просматривать текущую запись. Он имеет ограниченные права на перемотку и скачивание записи (на компьютер или другой носитель);
б) Право на перемотку и отслеживание записей камер видеонаблюдения - пользователь с данным доступом может осуществлять мониторинг камер в режиме реального времени, а также перематывать и отслеживать записи, но имеет ограниченные права на скачивание записи (на компьютер или другой носитель);
в) Загрузка записей с камер видеонаблюдения - пользователь, имеющий данный доступ, может осуществлять мониторинг камер в режиме реального времени, перематывать и отслеживать записи, загружать записи в локальную сеть и, при соответствующем подтверждении, передавать их уполномоченному лицу;
г) Право на техническую поддержку - пользователь, имеющий вышеуказанный доступ, имеет право создавать новых пользователей в системе видеонаблюдения, аннулировать существующих пользователей, осуществлять электронный контроль выполняемых действий (журналов) в системе видеонаблюдения, выполнять различные действия по устранению неисправностей в случае возникновения технических проблем, а также вносить изменения в конфигурацию.
Примечание: Пользователь — это любое лицо, имеющее доступ к системе видеонаблюдения. Доступ к системе видеонаблюдения возможен только по индивидуальному имени пользователя и паролю.

Статья 15 Сотрудник по защите персональных данных
1. В Университете функционирует ответственное лицо по защите персональных данных, которое обеспечивает соответствие процессов обработки персональных данных законодательству о защите персональных данных.
2. Уполномоченный по защите персональных данных независим в своей деятельности и подчиняется ректору Университета.
2. Сотрудник по защите персональных данных:
а) информирование лица, ответственного за обработку, лица, уполномоченного на обработку, и их работников по вопросам, связанным с защитой данных, в том числе о принятии или изменении нормативных правовых актов, а также оказание им консультационной и методической помощи;
б) участие в разработке внутренних нормативных актов и документов по оценке воздействия на защиту данных, связанных с обработкой данных, а также контроль за соблюдением лицом, ответственным за обработку, или лицом, уполномоченным на обработку, законодательства Грузии и внутренних организационных документов;
в) анализ поступивших заявлений и жалоб по вопросам обработки данных и выдача соответствующих рекомендаций;
г) получение консультаций от Службы по защите персональных данных, представление лица, ответственного за обработку, и лица, уполномоченного на обработку, в отношениях со Службой

по защите персональных данных, представление информации и документов по ее запросам, а также координация и контроль выполнения ее задач и рекомендаций;
д) предоставление информации о процессах обработки данных и правах субъекта данных по запросу;
е) выполнение лицом, ответственным за обработку, или лицом, уполномоченным на обработку, иных функций в целях повышения стандартов обработки данных.

Статья 16 Обновление политики
В случае изменения отдельных вопросов, связанных с обработкой данных, политика может быть обновлена по мере необходимости.