УТВЕРЖДЕНО
на заседании Сената ТГУ
(протокол № 11 от 13.06.2016 г.

Ректор университета
доц. д-р Мария Паслярь
«_13_» _06_ 2016 г.

П О Л О Ж Е Н И Е

об обработке информации, содержащей персональные данные, в системе бухгалтерского учета Тараклийского госуниверситета имени Григория Цамблака

Тараклия, 2016 г.

I. ОБЩИЕ ПОЛОЖЕНИЯ

1. Положение об обработке информации, содержащей персональные данные, в системе бухгалтерского учета (далее - Положение) разработано в целях реализации в Тараклийском госуниверситете имени Григория Цамблака, положений Закона №133 от 8 июля 2011 г. о защите персональных данных, Закона о бухгалтерском учете №113 от 27 апреля 2007 г. и Требований по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденных Постановлением Правительства №1123 от 14 декабря 2010 г., а также для соблюдения положений ст. 91-94 Трудового кодекса Республики Молдова.

2. Настоящее Положение регламентирует общие условия и требования к обработке персональных данных работников Тараклийского госунивенрситета им. «Гр.Цамблака» в системе бухгалтерского учета.

II. ЦЕЛЬ

1. Целью обработки информации, содержащей персональные данные, в системе бухгалтерского учета является обеспечение регистрации бухгалтерской информации, касающейся расчета заработной платы работников, в том числе премий, поощрений, надбавок, пособий, компенсаций и других прав и обязанностей материального характера, а также предоставления государственным учреждениям квартальных и годовых финансовых отчетов, в соответствии с действующим законодательством.

2. В системе бухгалтерского учета обрабатываются следующие категории персональных данных:

- фамилия, имя и отчество;
- персональный идентификационный номер (IDNP);
- дата рождения и место жительства;
- персональный код социального страхования (CPAS);
- сведения о месте работы и занимаемой должности;
- размер валового оклада и другие премии, надбавки, поощрения, доплаты;
- сведения о семейном положении (по запросу заинтересованного лица);
- фамилия, имя (если имеется, отчество) лиц, находящихся на содержании у данного лица (члены семьи, другие родственники, если таковые имеются);
- реквизиты банковского счета для перечисления заработной платы и других сумм, подлежащих выплате в качестве пособий, компенсации или других прибылей, по обстоятельствам;
- данные из полученных справок о медицинском отпуске, необходимые для исчислении соответствующего пособия;
- конкретный размер подсчитанных вознаграждений, соответствующие налоги и пошлины, включительно взносы за обязательное медицинское и социальное страхование, и другие суммы, подлежащие выплате на законной или договорной основе;
- по обстоятельствам, другие данные, необходимые для реализации вышеуказанной цели, в соответствии с действующим законодательством.

3. Обработка персональных данных осуществляется для реализации следующих целей:

a. Обработка информации об изменениях в обработке персональных данных, касающихся работников, которые влияют на расчет заработной платы, например: изменение уровня квалификации , повышение по ступеням оплаты труда, предоставление или отзыв допуска к государственной тайне, оценивание профессиональных достижений с установлением надбавки за стаж работы ;

b. Расчет месячной заработной платы, в соответствии с действующим законодательством Республики Молдова (Закон №355 от 23.12.2005 г. о системе оплаты труда в бюджетной сфере);

c. Обработка справок работников о медицинском отпуске для установления соответствующих пособий;

d. Обработка копий приказов ректора по персоналу;

e. Исчисление и удержание налогов из заработной платы работников: страховые взносы на обязательное медицинское страхование, взносы в бюджет государственного социального страхования, подоходный налог и т.д.;

f. Начисление и перечисление взносов на обязательное медицинское страхование и взносов в бюджет государственного социального страхования из заработной платы - обязанность работодателя;

g. Предоставление информации, необходимой для разработки ежеквартальных отчетов о взносах обязательного государственного социального страхования (форма 4BASS), и взносов на обязательное медицинское страхование (Форма MED08);

h. Подготовка ежеквартально декларации застрахованного лица REV 5 на каждого работника и их передача в Территориальную кассу социального страхования, филиал Тараклия в электронном формате посредством SIA E-REPORTING и, ежегодно, на бумажном носителе;

i. Содействие процессу (путем предоставления необходимой информации) для периодического (ежемесячного) заполнения докладов и отчетов о выплаченном доходе и удержанном из него подоходном налоге;

j. Ежемесячная, поквартальная и годовая подготовка отчетов и их представление в Государственную налоговую инспекцию Тараклия (о подоходном налоге IRV 09, TFD 10, IAL 09, MED 08), а также разработка и предоставление информации о доходах, начисленных и выплаченных в пользу физического лица, и о подоходном налоге, удержанном из этих доходов, работникам Тараклийского госуниверситета имени Григория Цамблака;

k. Обработка заявлений и подтверждающих документов о предоставлении освобождений по подоходному налогу, удержанному из заработной платы, в соответствии с главой 4 раздела II Налогового кодекса;

l. Выдача справок о заработной плате, по просьбе работников;

m. Заполнение и хранение личных карточек учета доходов в виде заработной платы и других выплат, осуществленных работодателем в пользу работника, на каждый год, а также подоходного налога, удержанного из этих выплат (Приложение №8 к Приказу ГГНИ №676 от 14.12.2007 г.)

4. Персональные данные, являющиеся предметом регулирования настоящего Положения хранятся в электронном и бумажном виде, позволяющем идентифицировать их субъектов только в течение времени, необходимого для достижения целей их обработки, а по истечению данного срока, записи должны быть уничтожены/удалены, в зависимости от типа носителя, на котором они были сделаны. При выполнении возложенных законом обязанностей, данные могут оставаться на хранении, приобретая статус архивного документа.

5. Любое использование персональных данных, введенных в систему бухгалтерского учета для целей, отличных от указанных выше, запрещается.

III. МЕСТО НАХОЖДЕНИЕ И ОПИСАНИЕ СИСТЕМЫ БУХГАЛТЕРСКОГО УЧЕТА

1.Персональные данные, содержащиеся в системе бухгалтерского учета Тараклийского государственного университета имени Григория Цамблака, обрабатываются/хранятся:

1. на бумажном носителе;

2.Обработка информации в системе бухгалтерского учета на бумажном носителе распределяется по критерию «папки-дела», последние хранятся в шкафах, расположенных в бухгалтерии госуниверситета.

IV. СРОК ХРАНЕНИЯ

4.1. Обработка персональных данных в системе бухгалтерского учета осуществляется в период действия договоров о государственных закупках, в период работы работников ТГУ (с момента подписания договора до момента завершения осуществления действий, предусмотренных законодательными актами в случае прекращения трудовых отношений).

4.2. После истечения сроков, указанных в пункте 4.1., данные из системы бухгалтерского учета подлежат архивному хранению в период, установленный Номенклатурой дел университета, а впоследствии подлежат уничтожению или удалению, в зависимости от типа носителя, на который они были записаны.

V. ПРАВА РАБОТНИКОВ И СУБЪЕКТОВ ДАННЫХ

5.1. Тараклийский госуниверситет имени Григория Цамблака, в качестве оператора персональных данных, гарантирует соблюдение прав на защиту персональных данных, которыми обладают работники и, по обстоятельствам, другие субъекты.

5.2. В соответствии с принципами защиты персональных данных, субъекты данных имеют следующие права: на информацию, на доступ к данным, на вмешательство, на возражение в отношении персональных данных, которые их касаются, а также право обратиться к правосудию.

5.3. Все лица, участвующие в управлении информацией системы бухгалтерского учета и/или ее обработке, должны соблюдать процедуру доступа к персональным данным.

5.4. Предоставление работникам права доступа к информации, которая их касается, осуществляется только по запросу, поданному в письменной форме, по согласованию непосредственно с ректором универистета. Информация должна быть предоставлена таким образом, чтобы не ущемлялись права третьих лиц. Лица, запрашивающие персональные данные, должны указать цель запроса, а также конкретный период, за который запрашивается информация.

5.5. В праве доступа может быть отказано в случае применения исключений, предусмотренных законом. Ограничение доступа может потребоваться и в случаях, когда необходимо защитить права и свободы третьих лиц, например, если запрошенная информация содержит данные о других лицах и нет возможности получить их согласие или когда, посредством редактирования, невозможно извлечь персональные данные не важные для заявителя.

VI. МЕРЫ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОБРАБАТЫВАЕМЫХ В СИСТЕМЕ БУХГАЛТЕРСКОГО УЧЕТА

1. Общие мероприятия по управлению информационной безопасностью.

1.1 В случае временного неиспользования бумажных и электронных носителей информации, содержащих персональные данные, они хранятся в запирающихся сейфах.

1.2 По окончании рабочих сессий, компьютеры и принтеры отключаются от источника электроэнергии.

1.3 Оператор обеспечивает безопасность пунктов приема и отправки корреспонденции, а также защиту против неавторизованного доступа к копировальным устройствам.

1.4 Физический доступ к средствам отображения информации, полученной из системы бухгалтерского учета, заблокирован с целью препятствования визуализации этой информации неавторизированными на это лицами.

1.5 Средства обработки информации, полученной из системы бухгалтерского учета, или программные обеспечения, предназначенные для их обработки, выносятся из периметра безопасности только на основании письменного разрешения оператора.

1.6 Вынос и внос средств обработки персональных данных системы бухгалтерского учета из периметра/в периметр безопасности должен регистрироваться в регистре.

2. Меры по защите персональных данных, обрабатываемых в системе бухгалтерского учета, применяются исходя из необходимости обеспечения конфиденциальности и целостности этих мер, посредством мануальной, электронной и внешней защиты.

3. Специальные требования к маркировке: вся информация, полеченная из системы бухгалтерского учета, которая содержит персональные данные, подлежит маркировке с указанием предписаний для их последующей обработки и распространения, в том числе с указанием единого идентификационного номера оператора персональных данных.

4. Доступ в кабинет, где расположена система бухгалтерского учета, ограничен и разрешен только лицам, имеющим необходимое разрешение, и только в рабочее время. Доступ в кабинет возможен только при наличии разрешения на доступ и ключа от механического замка.

5. Вход в кабинет всегда находится под наблюдением, дверь кабинета закрывается на замок.

6. До предоставления физического доступа к системе бухгалтерского учета, проверяются полномочия доступа.

7. Регистры мониторинга хранятся не менее одного года, по истечении указанного срока они ликвидируются, а данные и документы, содержащиеся в ликвидируемом регистре, передаются в архив.

8. Периметром безопасности считается периметр кабинета, в котором расположена система бухгалтерского учета, который должен быть целостным с физической точки зрения.

9. Периметр безопасности здания и кабинета, в котором расположена система бухгалтерского учета, проверяется ежедневно с физической точки зрения.

10. Компьютеры расположены в местах с ограниченным доступом для посторонних лиц.

11. Двери и окна запираются при отсутствии в помещении работников, уполномоченных управлять системой.

12. Расположение системы бухгалтерского учета соответствует необходимости обеспечения ее безопасности от несанкционированного доступа, краж, пожаров, наводнений и других возможных рисков.

13. Электроэнергетическая безопасность: обеспечивается безопасность электрооборудования, используемого для поддержания функциональности системы бухгалтерского учета, электрических кабелей, включая их защиту от повреждений и несанкционированного подключения. В случае возникновения исключительных, чрезвычайных или форс-мажорных обстоятельств должна быть обеспечена возможность отключения от электричества систем бухгалтерского учета, включая возможность отключения любого компонента IT.

14. Компьютеры, на которых физически расположена система бухгалтерского учета, оснащены UPS (источниками бесперебойного питания), которые используются для правильного закрытия рабочей сессии систем (коспонентов) в случае отключения от источника электроэнергии.

15. Безопасность кабельных сетей: сетевые кабеля, посредством которых осуществляется обработка персональных данных, полученных из системы бухгалтерского учета, защищены от несанкционированного подключения или повреждения. Высоковольтные кабели должны быть отделены от кабелей связи для исключения помех.

16. Пожарная безопасность системы бухгалтерского учета: кабинет, где расположена система бухгалтерского учета, оборудован средствами обеспечения пожарной безопасности и соответствует действующим требованиям и нормам пожарной безопасности.

17. Контроль установки и удаления компонентов IT: осуществляется контроль и учет установки и удаления программных, технических и программно-аппаратных средств, используемых в системе бухгалтерского учета. По истечению срока хранения, информация, содержащая персональные данные и хранящаяся на носителях информации, подлежит уничтожению.

VII. ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЯ СИСТЕМЫ БУХГАЛТЕРСКОГО УЧЕТА

1. Осуществляется идентификация и аутентификация пользователей информации, полученной из систем бухгалтерского учета и процессов, исполняемых от имени этих пользователей.

2. Все пользователи (включая персонал технической поддержки, администраторов сети, программистов и администраторов базы данных) имеют уникальный идентификатор (пользовательский ID), который не должен содержать признаков уровня доступа пользователя.

3. Для подтверждения заявленной идентичности пользователя используются пароли. Использование паролей в процессе обеспечения информационной безопасности: помимо требований по сохранению конфиденциальности паролей, запрещается их запись на бумажных носителях, если только не обеспечено их безопасное хранение (помещение записей в сейф). В момент ввода пароли не отображаются на экране.

4. Пароли меняются каждый раз, когда обнаруживаются признаки возможной компрометации системы или пароля.

5. Для обеспечения возможности установления ответственности каждого пользователя, используются их индивидуальные пароли и идентификаторы. Обеспечивается пользователям возможность выбирать и изменять собственные пароли, а также активировать процедуру для учета ошибочного ввода паролей. После трех ошибочных попыток аутентификации, доступ автоматически блокируется.

6. Обеспечивается хранение в течение 1 /одного/ года предыдущих историй паролей в форме hash и предотвращение их повторного использования.

7. В случае, если трудовые отношения пользователя были прекращены, приостановлены или изменены, а новые должностные обязанности не требуют доступа к персональным данным, а также в случае изменения права доступа пользователя, злоупотребления пользователем полученными разрешениями на доступ с целью совершения деяния, наносящего вред, в случае отсутствия пользователя на рабочем месте на протяжении продолжительного периода времени (более 3 месяцев), коды идентификации и аутентификации отзываются или приостанавливаются.

8. Посредством автоматизированных средств поддержки, осуществляется управление учетными записями пользователей, которые обрабатывают персональные данные в системе бухгалтерского учета, включая создание, активацию, изменение, пересмотр, отключение и удаление учетных записей. Действие учетных записей временных пользователей, которые обрабатывают персональные данные в системе бухгалтерского учета, автоматически прекращается по окончанию установленного периода времени (для каждого типа учетной записи в отдельности). Осуществляется автоматическое отключение учетных записей неактивных пользователей, которые обрабатывают персональные данные в системе бухгалтерского учета, после периода бездействия не более 1 */одного/* месяца. Используются автоматизированные средства регистрации и оповещения о создании, изменении, отключении, прекращении действия учетных записей.

9. В целях обнаружения и предотвращения случаев предоставления несанкционированных прав доступа, права доступа пользователей системы бухгалтерского учета пересматриваются регулярно, не более чем через каждые 6 месяцев и и после любых изменений статуса пользователя.

10. Использование беспроводных технологий, портативных и мобильных устройств авторизируется ответственными лицами.

11. Устанавливаются ограничения в отношении лиц, имеющих право:
a) просматривать информацию, сохраненную в системе бухгалтерского учета;
b) копировать, скачивать, удалять или изменять любую сохраненную информацию.

12. Все работники, имеющие право доступа, проходят начальную подготовку в области защиты персональных данных.

13. Любое действие по разглашению персональных данных третьим лицам документируется и предварительно подвергается строгому анализу в отношении цели и правовой основы намерений разгласить определенный объем персональных данных.

14. Любое нарушение безопасности в отношении системы учета подлежит документации, а лицо, ответственное за реализацию политики безопасности должно быть проинформировано об этом как можно быстре.

15. Перед предоставлением доступа в систему, пользователи информируются о том, что использование системы бухгалтерского учета контролируется и что ее неавторизированное использование наказывается в соответствии с гражданским законодательством, законодательством об административно-правовых нарушениях и уголовным законодательством.

VIII. АУДИТ БЕЗОПАСНОСТИ В СИСТЕМАХ БУХГАЛТЕРСКОГО УЧЕТА

1. Организуется генерирование записей аудита безопасности в системе бухгалтерского учета для событий, указанных в соответствующем списке, подвергаемых аудиту.

2. Осуществляется регистрация попыток входа пользователя в систему/выхода из системы по следующим параметрам:

a. дата и время попытки входа/выхода;
b. идентификатор пользователя;
c. результат попытки входа/выхода – успешная или безуспешная.

3. Осуществляется регистрация попытки запуска/завершения рабочей сессии прикладных программ и процессов, предназначенных для обработки информации из систем бухгалтерского учета, регистрация изменения прав доступа пользователя и статуса объектов доступа по следующим параметрам:
a. дата и время попытки запуска;
b. наименование/идентификатор приложения или процесса;
c. идентификатор пользователя;
d. результат попытки запуска – успешная или безуспешная.

4. Осуществляется регистрация попыток получения доступа (выполнения операций) к приложениям и процессам, предназначенным для обработки информации из систем бухгалтерского учета, по следующим параметрам
a. дата и время попытки получения доступа (выполнения операции);
b. наименование (идентификатор) приложения или процесса;
c. идентификатор пользователя;
d. спецификация защищаемого ресурса (идентификатор, логическое имя, имя файла, номер и т.п.);
e. вид запрашиваемой операции (чтение, запись, удаление и т.п.);
f. результат попытки получения доступа (выполнения операции) – успешная или безуспешная.

5. Осуществляется регистрация изменения прав доступа (полномочий) пользователя и статуса объектов доступа по следующим параметрам:
a. дата и время изменения полномочий;
b. идентификатор администратора, осуществившего изменения;
c. идентификатор пользователя и его полномочия или спецификация объектов доступа и их новый статус.

6. Осуществляется регистрация выхода из системы бухгалтерского учета, регистрация изменения прав доступа субъектов и статус объектов доступа по следующим параметрам:
a. дата и время выдачи;
b. наименование информации и пути доступа к ней;
c. спецификация оборудования (устройства) выдачи информации (логическое имя);
d. идентификатор пользователя, запросившего информацию;
e. объем выданного документа (количество страниц, листов, копий) и результат выдачи – успешный или безуспешный.

7. Случаи сбоя аудита безопасности в системе бухгалтерского учета или заполнения всего объема памяти, выделенного для хранения данных аудита, доводятся до сведения лица, ответственного за политику безопасности персональных данных, которое предпринимает действия по восстановлению работоспособности системы аудита.

8. Результаты аудита безопасности в системе бухгалтерского учета (операции по обработке персональных данных и средства для проведения аудита) защищаются от несанкционированного доступа путем установления надлежащих мер безопасности и обеспечения конфиденциальности и целостности этих результатов.

9. Минимальный срок хранения результатов аудита безопасности в системе бухгалтерского учета составляет 2 */два/* года, в целях обеспечения возможности их использования в качестве доказательств в случае инцидентов безопасности, возможного

расследования или судебных процессов. В случае, когда срок расследования или судебные процессы продлеваются, результаты аудита хранятся в течение всего этого срока.

IX. ОБЕСПЕЧЕНИЕ ЦЕЛОСТНОСТИ ИНФОРМАЦИИ СИСТЕМЫ БУХГАЛТЕРСКОГО УЧЕТА

1. Обеспечивается выявление, протоколирование и устранение недостатков программных обеспечений, предназначенных для обработки информации системы бухгалтерского учета, включая установку исправлений и пакетов обновлений для этих программ, защита от проникновения вредоносных программ в программное обеспечение, меры, которые обеспечивают возможность своевременного автоматического обновления средств, обеспечивающих защиту от вредоносных программных обеспечений и сигнатур вирусов.

2. Используются технологии и средства констатации незаконных вторжений, которые позволяют мониторизировать происшествия и констатировать атаки, в том числе те, которые обеспечивают выявление неавторизированных попыток использования информации системы бухгалтерского учета.

3. Обеспечивается тестирование правильного функционирования компонентов по обеспечению безопасности системы бухгалтерского учета (автоматически - при запуске системы и по необходимости - по запросу лица, ответственного за политику безопасности в отношении обработки персональных данных).

4. Резервные копии: исходя из объема выполненной обработки, оператором индивидуально определяется интервал времени, в котором выполняется резервное копирование информации системы бухгалтерского учета и программных обеспечений, использованных для ее автоматизированной обработки. Резервные копии тестируются для проверки безопасности носителей информации и целостности данной информации. Процедуры по восстановлению резервных копий актуализируются и тестируются регулярно в целях обеспечения их эффективности.

X. АДМИНИСТРИРОВАНИЕ ИНЦИДЕНТОВ БЕЗОПАСНОСТИ СИСТЕМЫ БУХГАЛТЕРСКОГО УЧЕТА

1. Лица, обеспечивающие эксплуатацию системы бухгалтерского учета, проходят не реже одного раза в год инструктаж в отношении ответственности и обязательств в случае выполнения действий по управлению и реагированию на инциденты безопасности.

2. Обработка инцидентов безопасности включает обнаружение, анализ, предотвращение развития, их устранение и восстановление безопасности. Проводится постоянный мониторинг и документирование инцидентов безопасности системы бухгалтерского учета.

3. Лица, виновные в нарушении норм, регулирующих получение, хранение, обработку и защиту информации системы бухгалтерского учета несут, гражданско-правовую, правонарушительную и уголовную ответственность.

XI. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

1. Настоящее Положение пересматривается и впоследствии утверждается ректором ТГУ периодически, но не реже одного раза в год, а также по необходимости.

2. Настоящее Положение дополняется положениями действующего законодательства.

3. Положение доводится до сведения работников под подпись.

4. Внесение изменений и дополнений в настоящее Положение осуществляется в порядке, предусмотренном для его утверждения.