УТВЕРЖДЕНО

приказом ректора

ОУ Европейский гуманитарный университет

№ 01-33 от 01.04.2019

ПРАВИЛА ОБРАБОТКИ ЛИЧНЫХ ДАННЫХ ОБЩЕСТВЕННОГО УЧРЕЖДЕНИЯ «ЕВРОПЕЙСКИЙ ГУМАНИТАРНЫЙ УНИВЕРСИТЕТ»

На основании того, что Регламент Европейского парламента и Совета (ЕС) 2016/679 О защите физических лиц в отношении обработки личных данных и о свободном движении таких данных, а также об отмене Директивы 95/46/ЕС (Общий регламент по защите данных) от 27 апреля 2016 года (далее – «Регламент») предусматривает администратору данных обязанность должным образом применять правильные технические и организационные средства для обеспечения безопасности личных данных, а также обязанность доказать что предприятие придерживается Регламента,

Общественное учреждение Европейский гуманитарный университет (далее и – «Университет» или «Администратор данных») утвердило данные правила обработки личных данных (далее – «Правила»).

Основные понятия

Администратор данных – ОУ Европейский гуманитарный университет, код юридического лица 300548028, адрес регистрации ул. Савичяус, 17, 01127 Вильнюс.

Сотрудник (-и) – лицо или лица, с которым (-и) Университет имеет трудовые, авторские договора или договора подряда на преподавание.

Инспекция – Институция для присмотра данных Литовской Республики Государственная инспекция защиты данных.

Другие понятия, используемые в настоящих Правилах, понимаются так, как они определены в Регламенте и иных правовых актах Литовской Республики, включая, но не ограничиваясь, Закон о правовой защите личных данных Литовской Республики (далее – «Закон»), Трудовой кодекс Литовской Республики, Гражданский кодекс Литовской Республики и др.

Содержание Правил:

I. ОБЩИЕ ПОЛОЖЕНИЯ

1. Правила подготовлены на основании положений Регламента, Закона, Трудового кодекса и иных правовых актов, регламентирующих защиту и обработку данных.
2. Правила применяются и являются обязательными для Администратора данных - Университета, и для всех сотрудников, работающих в данном Университете (включая и лиц, работающих по срочным, авторским договорам или договорам подряда), которые обрабатывают личные данные или узнают их, исполняя свои обязанности.
3. Правила публикуются в виртуальном офисе Университета, к которому имеют доступ все сотрудники и могут в любое время повторно с ними ознакомиться. В случае изменения положений данных Правил, специалист по защите данных Университета информирует об этих изменениях сотрудников не позже чем на следующий рабочий день после их утверждения.
4. В деятельности Администратора данных используются технические и организационные средства защиты данных, указанные в Общем списке технических, организационных и

физических средств. Данные средства устанавливаются в соответствие с характером данных, которые обрабатываются в Университете, и обеспечивают уровень защиты, соответствующий риску, который за собой влечёт обработка данных.

5. За политику обработки данных, осуществляемую в Университете, в пределах своей компетенции отвечает специалист по защите данных. Права, обязанности, роль и принципы деятельности специалиста по защите данных установлены в Положении о деятельности специалиста по защите данных.

II. ЦЕЛИ И ОБЪЕМ ОБРАБОТКИ ДАННЫХ

6. Цели обработки личных данных Университета устанавливает Ректор Университета и иные уполномоченные лица (руководители подразделений Университета).

7. Перед принятием решений, связанных с личными данными, Ректор Университета и иные уполномоченные лица консультируются со специалистом по защите данных.

8. Цели, группы субъектов обрабатываемых в Университете личных данных, конкретные обрабатываемые личные данные и сроки хранения данных представлены в записях деятельности по обработке данных Университета (1 приложение к Правилам). Один раз в год проводится проверка того, необходима все ещё ли обработка личных данных соответствующего объема для достижения установленных целей по обработке личных данных.

9. После обнаружения избыточных, неиспользуемых данных или данных, законное основание обработки которых утратило силу, об этом необходимо незамедлительно информировать Специалиста по защите данных.

10. После получения сообщения об избыточных данных или данных, обработка которых не имеет никакого законного основания, Ректор Университета или иное уполномоченное лицо принимает соответствующие меры для устранения возможного несоответствия обработки данных положениям Регламента и иных правовых актов, также вносит корректировки в записи деятельности по обработке данных. При необходимости и после оценки возможного объема избыточных данных перед принятием решений Ректор Университета или иное уполномоченное лицо консультируется со Специалистом по защите данных.

III. ПРИНЦИПЫ ОБРАБОТКИ ДАННЫХ

11. Администратор данных в своей деятельности обрабатывает данные придерживаясь следующих принципов:

11.1. данные собираются и обрабатываются в определённых и законных целях, установленных перед обработкой данных и далее не обрабатываемые способом, несовместимым с этими целями (соблюдение принципа ограничения цели);

11.2. данные обрабатываются на законном основании обработки данных: законные интересы Университета, исполнение требований законодательства, заключение и выполнение договоров и, если необходимо, согласие субъекта данных (соблюдение принципа законности);

11.3. данные обрабатываются точно, добросовестно, законно и прозрачно (соблюдение принципа законности, добросовестности и прозрачности);

11.4. обрабатываются точные и, если это необходимо для обработки данных, постоянно обновляемые данные; неточные или неполные данные поправляются, дополняются, уничтожаются или их обработка приостанавливается, принимаются все обоснованные меры для обеспечения того, чтобы неточные личные данные, принимая во внимание цели их обработки, незамедлительно удалялись бы или исправлялись (соблюдение принципа точности);

11.5. обрабатываются адекватные, правильные и только такие данные, которые необходимы для достижения целей, из-за которых они обрабатываются (соблюдение принципа уменьшения количества данных);

11.6. данные хранятся только в такой форме, чтобы личность субъектов данных можно было бы установить не дольше, чем это необходимо для целей, на основании которых эти данные были собраны и обрабатываются (соблюдение принципа ограничения сроков хранения);

11.7. данные обрабатываются таким способом, чтобы при применении соответствующих технических или организационных средств обеспечивался бы правильный уровень защиты личных данных, включая защиту от обработки данных без разрешения или незаконной обработки данных или неумышленной потери, уничтожения или порчи данных (соблюдение принципа единства и конфиденциальности).

12. Университет в своей деятельности также придерживается принципов приспособленной и стандартизированной защиты данных:

12.1. Ректор Университета и руководители подразделений Университета обеспечивают, чтобы специалист по защите данных получал информацию о каждой новой услуге, продукту и / или иной деятельности, необходимую для проведения правильной оценки.

12.2. Если новый продукт и / или услуга включает использование новых технологий или есть основание предполагать, что новая услуга / продукт может иметь большое влияние на приватность лиц и иные связанные права, Ректор Университета или руководитель подразделения Университета, который инициировал запуск нового продукта и / или услуги, поручают специалисту по защите данных или иному ответственному лицу провести оценку воздействия на защиту данных (в таком случае специалист по защите данных консультирует лицо, которое проводит оценку воздействия на защиту данных).

12.3. Услуга и / или продукт, связанные с личными данными, не предлагаются (не используются) пока не получена оценка специалиста по защите данных или, когда это необходимо, отчёт оценки воздействия на защиту данных и нет подтверждения о соответствии требованиям Регламента и иных связанных законов.

13. Сотрудники Университета, в пределах своей компетенции обрабатывая личные данные, обязаны придерживаться принципов обработки личных данных, установленных в данном разделе.

IV. ОБРАБОТКА ДАННЫХ. ЗАПИСИ ДЕЯТЕЛЬНОСТИ ПО ОБРАБОТКЕ ДАННЫХ

14. Личные данные в Университете обрабатываются автоматическим способом или в систематизированных сборах, с использованием средств обработки личных данных, внедренных в Университете. Данные хранятся в информационных системах, указанных в записях деятельности по обработке данных, а также на жёстких дисках компьютеров сотрудников Университета.

15. Данные в Университете собираются в порядке, установленном правовыми актами, получая их напрямую с субъекта данных, официально запрашивая необходимую информацию от субъектов, которые её обрабатывают и имеют право её предоставлять, или на основании договоров. При необходимости личные данные могут обрабатываться при наличии согласия субъекта данных.

Записи деятельности по обработке данных

16. Университет ведет записи деятельности по обработке данных, в которых указывается следующая информация об обработке личных данных, осуществляемой Университетом:

16.1. контактные данные администратора данных;

16.2. контактные данные специалиста по защите данных администратора данных;

16.3. цели обработки личных данных;

16.4. категории субъектов данных;

16.5. категории личных данных;

16.6. законное основание обработки личных данных;

16.7. сотрудники администратора данных, имеющие права доступа к личным данным;

16.8. категории получателей данных;

16.9. место хранения данных;

16.10. порядок информирования субъектов данных;

16.11. сроки хранения личных данных;

16.12. лица, ответственные за уничтожение личных данных по истечению срока их хранения;

16.13. применяемые технические и организационные средства безопасности (приводится ссылка на общее описание технических и организационных средств, утверждённое Университетом).

17. В случаях, когда администратор данных действует как обработчик данных, в записях деятельности по обработке данных, которые он ведёт, указывается следующая информация о его деятельности по обработке данных, осуществляемой им как обработчиком данных:

17.1. контактные данные обработчика данных;

17.2. контактные данные специалиста по защите данных обработчика данных;

17.3. контактные данные администраторов данных;

17.4. ссылки на договора с администраторами данных;

17.5. категории обработки личных данных;

17.6. место хранения личных данных;

17.7. получатели личных данных из третьих стран;

17.8. применяемые технические и организационные средства безопасности (приводится ссылка на документы, в которых устанавливаются данные средства).

18. За заполнение, проверку и обновление информации записей деятельности по обработке данных отвечает Специалист по защите данных.

19. Записи деятельности по обработке данных хранятся в виртуальном офисе Университета.

20. В случае если уполномоченное государственное учреждение предъявляет обоснованное требование ознакомится с записями деятельности по обработке данных, соответствующие записи в срок, указанный в заявлении, предоставляет Ректор Университета или другой сотрудник Университета по его поручению.

21. Записи хранятся в таком формате и в таком порядке, чтобы по требованию Государственной инспекции по защите данных требуемые записи можно было бы передать.

22. За заполнение записей деятельности по обработке данных отвечает специалист по защите данных администратора данных. В случае изменения информации, указанной в записях деятельности по обработке данных руководитель подразделения предприятия администратора данных или уполномоченное им лицо незамедлительно по электронной почте информирует специалиста по защите данных администратора данных об изменении.

23. Получив информацию об изменившихся данных, специалист по защите данных не позже чем на следующий день после получения информации выполняет следующие действия:

23.1. перед тем, как вносить соответствующие изменения, сохраняет вариант записей деятельности по обработке данных, действовавший до изменений, указывая в названии период, во время которого данный вариант записей деятельности по обработке данных был действителен (например, 2018-01-01–2018-05-31 ЗДОД);

23.2. вносит соответствующие изменения в записи деятельности по обработке данных.

24. Недействительные варианты записей деятельности по обработке данных хранятся 2 года после дня обновления записей деятельности по обработке данных.

V. ОБРАБОТЧИКИ ДАННЫХ И ПОЛУЧАТЕЛИ ДАННЫХ

Обработчики данных

25. Администратор данных может дать право обрабатывать свои данные обработчикам данных, т.е. поставщикам услуг информационных технологий и электронных связей, аудиторам, консультантам, охранным фирмам и иным лицам, которые обрабатываемые Администратором данных данные обрабатывают в целях, установленных Администратором данных, и следуя его указаниям.

26. Перед привлечением обработчика данных должна быть оценена его надёжность. Надёжными считаются те обработчики данных, которые гарантируют, что имеют достаточно экспертных знаний, ресурсов, надёжности для того, чтобы обеспечить безопасность обработки личных данных.

27. С обработчиками данных Администратор данных заключает письменные договора, в которых предусматривается, что обработчики данных обрабатывают данные только следуя указаниям Администратора данных. Данные договора и их содержание должны соответствовать требованиям Регламента, которые применяются для договоров между администраторами данных и обработчиками данных об обработке личных данных.

28. В договоре между Администратором данных и обработчиком данных должен устанавливаться порядок, на основании которого представителю Университета предоставляются полномочия для проверки того, как обработчик данных придерживается своих обязательств.

29. Список обработчиков данных, уполномоченных Администратором данных, указывается в записях деятельности по обработке данных. После заключения каждого нового договора с обработчиком данных, записи деятельности по обработке данных дополняются данными нового обработчика данных. Соответственно, после расторжения договора с обработчиком данных, по инициативе специалиста по защите данных вносятся требуемые изменения в записи деятельности по обработке данных.

30. Специалист по защите данных информирует руководителей структурных подразделений Университета и иных сотрудников, обязанности которых включают обработку личных данных. Информация доносится по электронной почте или иными принятыми в Университете способами не позже чем в течение 3 дней от замены обработчика данных.

Получатели данных

31. Данные, обрабатываемые Администратором данных, третьим лицам предоставляются при наличии согласия субъекта данных или иного законного основания предоставления данных.

32. Обо всех просьбах предоставить личные данные (однократных и многократных) до начала предоставления данных или отправки отказа в предоставлении данных информируется специалист по защите данных.

33. В случаях однократного и многократного предоставления данных о существовании законного основания предоставления данных, обрабатываемых Университетом, принимает решение специалист по защите данных.

34. В случае отсутствия законного основания на предоставление данных, обрабатываемых Университетом, об этом информируется лицо, которое запрашивает данные.

35. Получателями личных данных, которые обрабатывает Университет, могут быть физические и юридические лица, предъявившие Университету просьбу о предоставлении данных или с которыми подписаны договора о предоставлении данных, а также иные юридические лица, которым личные данные передаются в целях обеспечения законных интересов Университета или на ином законном основании (для правозащитных учреждений, судов, судебным приставам, нотариальным конторам, адвокатам и др.).

36. Личные данные сотрудников Университета могут предоставляться только государственным учреждениям и учреждениям местного управления, которые в порядке, установленном законодательством Литовской Республики, уполномочены обрабатывать личные данные (периодическое предоставление данных в Управление фонда социального страхования (Содра), Государственной налоговой инспекции при Министерстве финансов, территориальному отделению службы по администрированию военной службы и др.). Данные сотрудников Университета также могут предоставляться третьим лицам на основании подписанных договоров, например, с целью заказа для сотрудников Университета билетов для поездки во время их командировок и др.

37. Данные, которые обрабатывает Университет, получателям данных за пределами Европейского экономического пространства предоставляются только в случае обеспечения ими должной степени правовой защиты данных (например, на основе стандартных требований договоров ЕС, системы «Privacy Shield», решений Европейской Комиссии об адекватной защите данных и др.) или, если нет иного законного основания, после получения разрешения Инспекции.

38. Список получателей личных данных, которые обрабатывает Администратор данных, представлен в записях деятельности по обработке данных.

VI. ПРАВА СУБЪЕКТОВ ДАННЫХ

39. Субъект данных (включая Сотрудников), данные которого обрабатываются в деятельности Администратора данных, при наличии основания, указанного в Регламенте, имеет следующие права:

39.1. знать (быть информированным) об обработке своих данных (право знать);

39.2. ознакомится со своими данными и тем, как они обрабатываются (право ознакомится);

39.3. требовать исправить или, принимая во внимание цели обработки личных данных, дополнить свои неточные личные данные (право исправить);

39.4. требовать удалить связанные с ним личные данные (право “быть забытым”);

39.5. требовать, чтобы Администратор данных ограничил обработку личных данных (право ограничить);

39.6. в любое время не согласится с обработкой своих личных данных, когда такая обработка осуществляется в целях общественного интереса или обработка данных необходима для достижения законных интересов Администратора данных или третьей стороны (право не согласиться);

39.7. получать связанные с ним данные, которые он предоставил Администратору данных, в систематизированном, обычно используемом и читабельном на компьютере формате и пересылать их другому администратору данных (право на переносимость данных);

39.8. право направить жалобу в Инспекцию.

40. Администратор данных может не создавать субъектам данных условий на осуществление прав, указанных в настоящем разделе, только в тех случаях, когда это необходимо для обеспечения превенции, расследования и обнаружения преступлений, нарушений служебной или профессиональной этики, а также для обеспечения защиты прав и свобод субъекта данных или иных лиц.

VII. ПОРЯДОК ОСУЩЕСТВЛЕНИЯ ПРАВ СУБЪЕКТОВ ДАННЫХ

41. Субъект данных может осуществить свои права только тогда, когда он создает Администратору данных возможность подтвердить его личность.

42. Личность субъекта данных подтверждается одним из ниже перечисленных способов:

42.1. субъекту данных прибыв по адресу Администратора данных и вместе с заявлением на осуществление прав предоставив документ, удостоверяющий личность (паспорт, карточку тождества личности или водительское удостоверение);

42.2. субъекту данных подтвердив свою личность в порядке, установленном правовыми актами, или используя электронные средства связи, которые позволяют правильно идентифицировать лицо (например, предоставив заявление, подписанное электронной подписью).

43. Сотрудники Администратора данных обязаны устно проинформировать субъектов данных, которые обращаются с просьбами осуществить права субъекта данных, о вышеперечисленных способах подтверждения личности.

Осуществление права знать (быть информированным)

44. Администратор данных, стремясь обеспечить должное осуществление права знать, а также обязательное осуществление добросовестности и прозрачности обработки личных данных, обязуется, что:

44.1. Во время передачи данных субъекту данных будет предоставлена вся ниже представленная информация, если этой информации у лица еще нет:

44.1.1. данные об идентичности Администратора данных (официальное название юридического лица и код юридического лица);

44.1.2. контактная информация Администрация данных (адрес регистрации, контактный номер телефона, адрес электронной почты);

44.1.3. контактные данные специалиста по защите данных (контактный номер телефона, адрес электронной почты);

44.1.4. цели обработки данных, на основании которых обрабатываются личные данные;

44.1.5. законное основание обработки данных;

44.1.6. конкретные законные интересы в тех случаях, когда личные данные обрабатываются на основании законных интересов Администратора данных или третьей стороны;

44.1.7. при передаче личных данных получателям данных указываются получатели данных или их категории;

44.1.8. в случае если планируется передача данных третьей стороне или международной организации – информация о намерении передать и о том, соответствует ли третья сторона или международная организация указанным в Регламенте требованиям защиты, и способы того, как можно получить информацию о соответствии;

44.1.9. срок хранения личных данных или, если это невозможно, критерии, применяемые к установлению этого срока;

44.1.10. информация о правах субъекта данных;

44.1.11. информация о том, является ли предоставление личных данных требованием, основанным на правовых актах или договорных обязательствах, или требованием, которое необходимо выполнить для заключения договора, а также о том, обязан ли субъект данных предоставить личные данные, и информация о возможных последствиях в случае не предоставления таких данных;

44.1.12. информация о том, что применяется автоматизированное принятие решений, включая профилирование, и смысловая информация о его логическом обосновании, а также смысл такой обработки данных и намечаемые последствия субъекту данных.

44.2. В случаях, когда личные данные поступают не от субъекта данных, администратор данных предоставит субъекту данных всю информацию, перечисленную в выше сформулированном подпункте Правил, а также ниже перечисленную информацию:

44.2.1. категории соответственных личных данных;

44.2.2. источник происхождения личных данных и, если применимо, получены ли данные из общедоступных источников.

44.3. Администратор данных указанную в настоящем пункте информацию представит:

44.3.1. в течение обоснованного периода с момента получения личных данных, но не позже как через один месяц, принимая во внимание конкретные обстоятельства обработки личных данных;

44.3.2. если личные данные будут использоваться для поддержания связи с субъектом данных - не позже чем во время первого контакта с этим субъектом данных;

44.3.3. если планируется передача личных данных другому получателю данных – не позже чем в первый раз раскрытия данных.

45. Конкретные способы информирования субъектов данных об обработке данных указаны в Записях деятельности об обработке данных.

46. Если администратор данных будет намерен дальше обрабатывать личные данные с иной целью, нежели та, с которой личные данные были получены, перед началом дальнейшей обработки тех данных администратор данных предоставит субъекту данных информацию об этой иной цели и всю дополнительную соответствующую информацию.

<u>Порядок осуществления права ознакомится с данными</u>

47. Осуществляя право ознакомится, субъект данных может направить запрос Администратору данных и получить от него информацию:

47.1. из каких источников и какие его данные собраны, если данные собираются не от субъекта данных;

47.2. с какой целью они обрабатываются;

47.3. каким получателям данных или принадлежащим к каким категориям получателям его данные были предоставлены хотя бы раз за последние два года или будут предоставляться;

47.4. о сроках хранения или, если это невозможно, о критериях, на основании которых устанавливается срок хранения;

47.5. о праве просить Администратора данных исправить или удалить данные или ограничить обработку личных данных, связанных с субъектом данных, или не согласится с такой обработкой;

47.6. о представлении данных третьим странам;

47.7. о том, что данные обрабатываются способом автоматизированного принятия решений, о смысле такой обработки и последствиях для субъекта данных.

48. Информация субъекту данных предоставляется после подтверждения личности субъекта данных. Получив запрос субъекта данных об обработке его данных, в течение 30 (тридцати) календарных дней со дня обращения субъекта данных Администратор данных ответит, обрабатываются ли связанные с ним данные и предоставит субъекту данных копию запрашиваемых личных данных. За любые другие запрашиваемые субъектом данных копии администратор данных может брать обоснованную плату, которая устанавливается по административным расходам (расходы на оказание услуги).

49. В случае если субъект данных отправляет запрос об обработке его личных данных по электронным каналам, информация предоставляется в общепринятой электронной форме, за исключением случаев, когда субъект данных просит предоставить ее иначе.

Порядок осуществления права требовать исправить личные данные

50. Если субъект данных думает, что связанные с ним данные неточные, он может обратиться к Администратору данных, а последний незамедлительно проверяет данные и, по просьбе субъекта данных, исправляет неточные данные.

51. Принимая во внимание цели, для достижения которых обрабатываются личные данные, субъект данных имеет право предоставить дополнительное заявление и потребовать, чтобы связанные с ним неполные личные данные были бы дополнены.

52. Неточные данные должны быть исправлены не позже чем в течение 15 (пятнадцати) рабочих дней со дня получения заявления от субъекта данных. Неполные данные должны быть дополнены не позже чем в течение 15 (пятнадцати) рабочих дней со дня получения заявления субъекта данных о конкретных дополнениях.

53. Коррекционные действия по исправлению и (или) дополнению данных инициирует специалист по защите данных. За исправление данных и (или) их дополнение отвечают сотрудники Университета, обрабатывающие данные, которые необходимо дополнить или исправить.

54. После исправления и (или) дополнения личных данных администратор данных сообщает об этом субъекту данных как можно быстрее по указанным им контактам. За информирование субъекта данных отвечает специалист по защите данных.

Порядок осуществления права требовать удалить данные (“быть забытым”)

55. В случае существования одной из ниже перечисленных причин субъект личных данных имеет право требовать, чтобы Администратор данных незамедлительно удалил бы связанные с ним личные данные:

55.1. личные данные больше не нужны для того, чтобы были достигнуты цели, для которых они собирались или иначе обрабатывались;

55.2. субъект данных отзывает согласие, которое является основанием обработки данных, и нет никакого иного законного основания для обработки данных;

55.3. субъект данных не соглашается с обработкой данных, и нет высших законных причин для обработки данных, или субъект данных не соглашается на использование данных в целях прямого маркетинга;

55.4. личные данные обрабатывались незаконно;

55.5. личные данные должны быть удалены на основании законной обязанности, установленной в законодательстве ЕС или Литовской Республики;

55.6. личные данные были собраны в контексте предложения услуг информационного общества.

56. После получения просьбы субъекта данных на осуществление права быть забытым, специалист по защите данных оценивает обоснованность такой просьбы.

57. При наличии хотя бы одного из выше перечисленных обстоятельств и после подтверждения личности субъекта данных, Администратор данных незамедлительно, но не позднее чем в течение 30 (тридцати) календарных дней со дня получения заявления с просьбой осуществить право на забвение, осуществляет данное право субъекта данных. За осуществление данного права субъекта данных отвечает специалист по защите данных.

58. После уничтожения личных данных администратор данных сообщает об этом субъекту данных как можно быстрее по указанным им контактам. За информирование субъекта данных отвечает специалист по защите данных.

Порядок осуществления права ограничить обработку данных

59. Субъект данных может требовать ограничить обработку данных, если:

59.1. субъект данных оспаривает точность данных на такой срок, в течение которого администратор данных может проверить точность личных данных;

59.2. обработка личных данных не является законной и субъект данных не соглашается на удаление данных, а вместо этого просит ограничить их использование;

59.3. личные данные Администратору данных в целях их обработки больше не нужны, но они необходимы субъекту данных для предъявления, осуществления или защиты правовых требований;

59.4. субъект данных возразил против обработки данных пока не будет проверено, являются ли законные причины Администратора данных выше причин субъекта данных.

60. После ограничения обработки личных данных Администратор данных может далее осуществлять действия по обработке личных данных за исключением хранения, только получив предварительное согласие субъекта данных или с целью предъявить, осуществить или защитить правовые требования или защитить личные права другого физического или юридического лица или по важным причинам общественного интереса.

61. Администратор данных незамедлительно информирует субъекта данных о том, что ограничение на обработку данных будет отменено.

62. За информирование субъекта данных отвечает специалист по защите данных.

Порядок осуществления права не согласиться

63. Субъект данных имеет право в любое время не согласится с тем, чтобы его личные данные обрабатывались бы, и Администратор данных больше не обрабатывает личные данные, когда такая обработка данных осуществляется:

63.1. для выполнения задачи, выполняемой во благо общественного интереса, или выполнения функций публичной власти, возложенных на Администратора данных;

63.2. для осуществления законных интересов администратора данных или третьей стороны.

64. После получения заявления субъекта данных о несогласии с тем, чтобы связанные с ним личные данные обрабатывались бы, специалист по защите данных оценивает обоснованность такого заявления и проводит оценку того, обрабатываются ли данные субъекта данных на законных убедительных основаниях.

65. Администратору данных доказав, что данные обрабатываются на убедительных законных основаниях, которые являются высшими над интересами, правами и свободами субъекта данных, или с целью предъявить, осуществить или защитить правовые требования, личные данные могут обрабатываться дальше.

66. После установления, что законных причин для обработки данных нет или недостаточно, личные данные дальше обрабатываться не должны.

67. В случае если личные данные обрабатываются в целях прямого маркетинга, субъект данных имеет право в любое время не согласиться с тем, чтобы связанные с ним личные данные обрабатывались бы в целях такого маркетинга, включая профилирование, насколько оно связано с таким прямым маркетингом.

68. Субъект данных об этом праве должен быть понятно проинформирован не позже чем в во время первого контакта с субъектом данных и данная информация представляется ясно и отдельно от всей остальной информации.

69. Если субъект данных возражает против обработки данных в целях прямого маркетинга, личные данные в таких целях больше не обрабатываются.

Порядок осуществления права на переносимость данных

70. В случаях, когда субъект данных предоставил данные Администратору данных в общепринятом и читабельном на компьютере формате, субъект данных имеет право получить эти данные и право требовать переслать те данные другому администратору данных, а Администратор данных не имеет права этому препятствовать когда:

    70.1. обработка данных основывается на согласии субъекта данных или необходимости обрабатывать личные данные для осуществления договора, стороной которого является субъект данных, или по его просьбе взяться за действия перед заключением договора; и

    70.2. данные обрабатываются используя автоматизированные средства.

71. При присутствии вышеуказанных обстоятельств и после подтверждения личности субъекта данных, по просьбе субъекта данных личные данные пересылаются напрямую другому администратору данных, но только в том случае если есть совокупность следующих обстоятельств:

    71.1. субъект данных указывает контакты нового администратора личных данных;

    71.2. пересылка данных технически осуществима.

72. Если нет хотя бы одного из вышеперечисленных обстоятельств, личные данные передаются лично субъекту данных в виде записи их на жёсткий носитель информации.

73. Осуществление права на переносимость личных данных не может нарушать или влиять на права и свободы других лиц.

* * *

74. За осуществление всех прав субъекта данных, указанных в настоящих Правилах, отвечает специалист по защите данных и все сотрудники Администратора данных в пределах своих компетенций.

75. Если личные данные субъекта данных, подавшего обоснованное заявление об осуществлении своих прав, от имени Администратора данных обрабатывают обработчики данных, Администратор данных обращается к ним и информирует о просьбе субъекта данных. Администратор данных контролирует, чтобы обработчики данных как можно быстрее помогли Администратору данных осуществить права субъекта данных и информировали бы Администратора данных о том, что права субъекта данных осуществлены в объёме личных данных, обрабатываемом обработчиком данных.

VIII. ПОРЯДОК УПРАВЛЕНИЯ НАРУШЕНИЯМИ БЕЗОПАСНОСТИ ЛИЧНЫХ ДАННЫХ И РЕАГИРОВАНИЯ НА ЭТИ НАРУШЕНИЯ

76. Администратор данных обеспечивает правильный мониторинг, определение и оценку нарушений безопасности личных данных. Факторы риска нарушения безопасности личных данных могут быть:

76.1. неумышленные, когда безопасность личных данных нарушается из-за случайных причин (ошибки обработки данных, перебои удаления, уничтожения информации и ее носителей, записей данных, установления неправильных маршрутов (адресов) при передаче данных и т.п. и систем из-за срыва поставки электричества, компьютерных вирусов и т.п., нарушение правил внутреннего распорядка, нехватка системного ухода, тестирование программного обеспечения, неподходящий уход за носителями данных, неподходящая мощность и защита линий, интеграция компьютеров в сеть, защиты компьютерных программ, недостаточная поставка факсовых материалов и др.);

76.2. умышленные, когда безопасность личных данных нарушается осознанно (незаконное вторжение в помещения, хранилища носителей личных данных, информационные системы, компьютерную сеть Университета, злостное нарушение установленных правил при обработке личных данных, сознательное распространение компьютерных вирусов, кража личных данных, незаконное использование прав другого сотрудника и др.);

76.3. внезапные случайные происшествия (молния, пожар, потоп, наводнение, бури, возгорание электрической инсталляции, воздействие изменений температуры и/или влажности, влияние грязи, пыли и магнитных полей, случайные технические аварии, иные непреодолимые и/или неконтролируемые факторы и пр.).

77. Нарушением безопасности личных данных считается происшествие, которое влечет за собой или может влечь за собой, среди прочего:

77.1. предание гласности личных данных;

77.2. утечку личных данных, т.е. когда личные данные становятся доступными лицам, у которых нет права их обрабатывать;

77.3. неисправности оборудования, используемого для обработки личных данных, которые могут повлечь за собой уничтожение личных данных;

77.4. ошибки личных данных.

78. Каждый сотрудник Университета, заметивший инцидент безопасности, обязан незамедлительно информировать о нем специалиста по защите данных Университета. Обязанность сотрудника сообщить об инциденте безопасности имеет преимущество над всеми остальными обязанностями сотрудника Университета, а промедление сотрудника сделать такое сообщение или не предоставление сообщения не могут быть оправданы никакими причинами, включая, но не ограничиваясь, выполнением более важных задач, отсутствием руководителей, отпуском или иными причинами.

79. Специалист по защите данных должен быть проинформирован обо всех инцидентах безопасности, включая, но не ограничиваясь, случаями, когда:

79.1. теряется или иными способами утрачивается компьютерное оборудование (компьютер, мобильный телефон и т.п.), карта памяти, USB носитель, внешний жёсткий диск или иной носитель данных, бумажные документы, в которых предположительно могут быть зафиксированы личные данные;

79.2. в помещениях или территории предприятия администратора данных находится оставленное без присмотра компьютерное устройство, носитель данных или бумажные документы;

79.3. при отправке электронного письма указывается неправильный адресат, т.е. вписывается адрес электронной почты не того лица, кому предназначается письмо;

79.4. при отправке электронного письма нескольким не связанными между собой адресатам за пределами предприятия администратора данных все получатели указываются в поле «кому / to» или «копия / cc», а не «невидимая копия / bcc»;

79.5. по электронной почте высылается незашифрованный и иным способом не защищённый файл данных с личными данными специальных категорий (например, медицинскими данными);

79.6. на ящик электронной почты или иную программу для общения, внедренную в предоставленном администратором данных устройстве, приходят подозрительные электронные письма, т.е. письма, отправитель которых предположительно прикидывается иным лицом, адрес электронной почты очевидно ненадёжный, в письме копируются товарные знаки, стиль иных лиц, в них присутствуют просьбы нажать подозрительные ссылки, скачать приложенные файлы с данными и т.п.;

79.7. антивирусная программа выдает сообщение об обнаруженных вирусах, червях, иных вредоносных программах или любой другой опасности для системы используемого устройства;

79.8. замечена подозрительная деятельность в компьютере или ином устройстве, предоставленном администратором данных: замедляется работа устройства, устройство или работающие на нем программы начинают само собой перезагружаться, выскакивают нежеланные окна, меняются настройки устройства и пр.;

79.9. не получается подключится к информационным системам администратора данных используя правильные данные авторизации;

79.10. уничтожаются актуальные и нужные личные данные и нет возможности самостоятельно их восстановить: удаляются сообщения электронной почты, данные, которые хранятся в компьютерах или иных устройствах, уничтожаются бумажные документы и т.п.

80. После проведения первичной оценки инцидента по нарушению данных, специалист по защите данных, принимая во внимание серьёзность инцидента по нарушению данных и возможное воздействие на права субъекта данных, незамедлительно осуществляет нижеуказанные действия:

80.1. формирует команду по расследованию инцидента данных и устранению последствий (не позже чем через 1 рабочий день после того дня, когда он узнал о нарушении);

80.2. прибегает ко всем возможным (принимая во внимание технологические и финансовые возможности) действиям для восстановления утерянных личных данных и / или уменьшения ущерба, который инцидентом по нарушению данных был причинён личным данным;

80.3. при необходимости обращается в государственные учреждения (полиция, Служба по регулированию связей, Национальный центр кибернетической безопасности и др.) (не позже чем через 1 рабочий день после установления потребности обратиться в соответствующее учреждение);

80.4. идентифицирует все группы личных данных, на которые может оказывать воздействие такой же инцидент по нарушению данных (не позже чем через 2 рабочих дня после того дня, как он узнал о нарушении);

80.5. принимает решение о необходимости сообщить об инциденте в Государственную инспекцию по защите данных (сообщать нет необходимости, если произошедшее нарушение не должно вызывать опасности для прав и свобод физических лиц);

80.6. установив, что нарушение безопасности данных может вызывать опасность правам и свободам физических лиц, поэтому необходимо сообщить о нем в Инспекцию, необходимо сделать это не позже чем в течение 72 часов с момента выяснения о нарушении безопасности данных. Сообщение в Инспекцию предоставляется путём заполнения типовой формы сообщения, утвержденной директором Инспекции, и: *(а)* отправки формы, подписанной электронной подписью, на адрес электронной почты ada@ada.lt с требованием подтвердить факт получения электронного письма; *(б)* предоставления сообщения через систему э-услуг Инспекции.

80.7. оценивает, может ли из-за этого нарушения безопасности личных данных возникнуть серьёзная опасность правам и свободам физических лиц и нужно ли информировать субъектов данных, данные которых были повреждены;

80.8. в случае установления, что из-за нарушения безопасности данных правам и свободам субъектов данных может возникнуть большая опасность, поэтому субъектов данных необходимо известить, инициирует поспешное информирование субъектов данных, данные которых были нарушены (за исключением случаев, предусмотренных в Регламенте, когда извещать о нарушении субъектов данных нет необходимости или дозволено публиковать извещение публично). В таком случае сам специалист по защите данных самостоятельно или уполномоченное им лицо готовит сообщение и без надобности не откладывая извещает каждого субъекта данных, на личные данные которого было оказано воздействие, об инциденте по нарушению данных для того, чтобы он смог принять должные меры его для пресечения. В сообщении должно быть перечислено, по крайней мере:

80.8.1. контактные данные специалиста по защите данных;

80.8.2. описан характер нарушения безопасности данных и возможные его последствия;

80.8.3. приведены рекомендации, предназначенные соответствующему физическому лицу, как удалить нарушение безопасности данных или возможное негативное его воздействие и последствия (например, блокировка писем с определённых адресов электронной почты и похожие действия);

80.9. оценив ситуацию в публичном пространстве и необходимость, инициирует подготовку сотрудниками Университета, ответственными за публичные связи, публичного объявления Администратора данных об инциденте по нарушению данных;

80.10. при необходимости без промедления обращается к третьим сторонам, которые могут помочь совладать с последствиями нарушения данных (поставщикам услуг ИТ, безопасности, помещений и ремонта техники и т.п.).

81. О каждом нарушении безопасности, которое признается нарушением безопасности личных данных, обязательно информируется Ректор Университета, также каждое такое нарушение в обязательном порядке должно быть зарегистрировано в журнале регистрации нарушений безопасности личных данных, который является частью Записей деятельности по обработке данных.

IX. ОБУЧЕНИЕ СОТРУДНИКОВ. ДОСТУП К ЛИЧНЫМ ДАННЫМ. СПЕЦИФИКА ОБРАБОТКИ ДАННЫХ СОТРУДНИКОВ

82. Все принимаемые на работу в Университет лица перед началом выполнения трудовых обязанностей должны быть ознакомлены с настоящими Правилами и иными внутренними (локальными) правовыми актами, регламентирующими работу с личными данными, а также подписать Декларацию конфиденциальности. Всем принятым на работу в Университет лицам в течение 7 дней со дня подписания договора проводится обучение на тему процессов обработки личных данных, во время которого им дополнительно разъясняются положения настоящих Правил, правила, связанные с поведением сотрудников в Интернет пространстве, указываются технические и административные средства, которые должен применять каждый конкретный сотрудник, а также другая важная информация. Обучение, среди прочего, охватывает разъяснение основных понятий (администратор данных, обработчик данных, субъект данных, личные данные, обработка данных, специальные личные данные), а также основных требований к обработке личных данных.

83. Сотрудники Университета обязаны придерживаться обязанности конфиденциальности и держать в тайне любую информацию, связанную с личными данными, с которой они ознакомились при исполнении своих обязанностей, если только такая информация не является публичной на основании положений действующих законов или иных правовых актов.

84. Принимая во внимание реальные потребности Университета, специалист по защите данных консультирует, информирует сотрудников Университета по вопросам защиты данных и организует их обучение.

85. Любой сотрудник Университета, у которого возникают подозрения, что технические и организационные средства безопасности, применяемые в Университете, не обеспечивают безопасность обрабатываемых в Университете данных, об этом незамедлительно извещает специалиста по защите данных или своего непосредственного руководителя.

Права доступа к личным данным, обрабатываемым в Университете

86. Права доступа и полномочия на обработку личных данных даются только тем сотрудникам Администратора данных, которым личные данные необходимы для выполнения их должностных обязанностей.

87. Уполномоченные сотрудники Администратора данных с личными данными могут проводить только те действия, на которые им даны права.

88. Сотрудникам Администратора данных дает, упраздняет и меняет права и полномочия доступа для обработки данных Ректор Университета или другой уполномоченный сотрудник по его поручению.

89. После окончания трудовых отношений Университета и сотрудника, в случае изменения трудовых обязанностей, для выполнения которых права доступа и полномочия на обработку личных данных не нужны, а также по истечению действия договора об обработке данных с обработчиком данных, права доступа и полномочия на обработку личных данных отменяются. Список лиц, которым Администратор данных предоставил право обрабатывать личные данные в Университете, и список их обязанностей представлен в Записях деятельности по обработке данных.

Специфика обработки данных сотрудников

90. К обработке данных сотрудников в Университете применяются те же принципы и положения как и к обработке данных иных категорий субъектов данных, за исключением упомянутых в настоящем разделе Правил специфических положений, которые применяются только к сотрудникам.

91. Университет подтверждает, что не обрабатывает личных данных сотрудников, не связанных с трудовыми отношениями (избыточных), также не предоставляет личных данных сотрудников третьим лицам, за исключением случаев, предусмотренных в настоящих Правилах или законодательстве.

92. Личные данные сотрудников Университета будут обрабатываться только на следующих законных основаниях:

92.1. исполнение трудового договора (выплата зарплаты и пр.);

92.2. осуществление законных повинностей, применяемых к Администратору данных (осуществление требований безопасности труда, уплата налогов и т.п.);

92.3. для достижения законных интересов Администратора данных или третьей стороны, за исключением случаев, когда такие интересы или основные права и свободы субъекта данных, из-за которых необходимо обеспечить защиту личных данных, являются за них выше;

92.4. в определённых исключительных случаях личные данные сотрудников могут обрабатываться с согласия сотрудника.

93. Срок хранения личных данных сотрудников устанавливается следуя соответствующим требованиям законодательства Литовской Республики. Личные данные сотрудников, не подлежащие хранению после окончания трудовых отношений, незамедлительно уничтожаются. За их уничтожение отвечают сотрудники, указанные в Записях деятельности по обработке данных.

94. В тех случаях, когда личные данные сотрудников обрабатываются на правовом основании законного интереса, специалист по защите данных проводит отдельную оценку обработки личных данных сотрудников на основании законного интереса, во время которой оценивается:

- необходима ли обработка личных данных для достижения законного интереса Университета или третьей стороны, нет ли альтернативных действий, которыми, не собирая личных данных сотрудника, можно было бы удовлетворить законные интересы Университета или третьей стороны;

- обеспечивает ли планируемая обработка личных данных баланс между интересами Университета или третьей стороны и правами и свободами сотрудника, т.е. все ли собираемые личные данные необходимы.

95. В случае если после проведения оценки устанавливается, что планируемая обработка личных данных для конкретной цели не является необходимой для достижения законного интереса и (или) планируемая обработка личных данных не обеспечит баланс между интересами Университета или третьей стороны и сотрудника, личные данные сотрудников на таком основании «законных интересов» не обрабатываются.

X. ДРУГИЕ ТРЕБОВАНИЯ ПО ОБРАБОТКЕ ДАННЫХ

96. Университет данные обрабатывает не дольше, чем это необходимо для достижения целей обработки данных. Сроки хранения данных предусмотрены в Записях деятельности по обработке данных.

97. Когда личные данные больше не нужны для достижения целей их обработки, они уничтожаются, за исключением тех данных, которые в случаях, предусмотренных законодательством, должны передаваться в государственные архивы, регистры и т.п.

98. Ненужные данные, собранные неавтоматизированным способом, ответственное за их обработку лицо уничтожает путём измельчения их шредером для документов, а данные, собранные автоматизированным способом, должны быть уничтожены путём удаления документов с ненужными собранными данными из среды хранения так, чтобы их невозможно было восстановить.

99. Ящик электронной почты каждого сотрудника считается базой личных данных, поэтому, во избежание избыточной обработки личных данных, сотрудники, работающие в Университете, отвечают за администрирование своего ящика электронной почты так, чтобы личные данные из электронных писем переносились бы в иные среды хранения или переписывались бы в трудовые договора, приказы ректора или иные документы и только в таком объёме, насколько это необходимо для достижения целей Администратора данных, а личные данные из электронных писем удалялись бы. Сотрудники ответственны за то, чтобы в ящиках их электронной почты не было бы писем старше трёх лет.

100. При отправке личных данных по электронной почте необходимо использовать безопасный канал, например, отправлять зашифрованный документ с личными данными и отправлять пароль к нему в другом письме.

XI. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

101. За согласование Правил с органом, представляющим сотрудников (Трудовой совет или профсоюз), и их утверждение ответствен Ректор Университета. За осуществление Правил, контроль над их применением, обновление, проведение иных действий, перечисленных в настоящих Правилах, отвечает Ректор Университета или назначенный им сотрудник в пределах своей компетенции.

102. Правила входят в силу после утверждения их Ректором Университета.

103. Правила пересматриваются и, при необходимости, обновляются после изменений правовых актов, регламентирующих защиту личных данных, но не реже чем один раз в два года.

104. Последний раз настоящие Правила были пересмотрены 1 апреля 2019 г.