Частное образовательное учреждение высшего образования
«Международный Институт Дизайна и Сервиса»
(ЧОУВО МИДиС)

УТВЕРЖДЕНО
приказом Ректора
от 31.08.2022 № 10-01-02/265

_____ М.В. Усынин

ПОЛОЖЕНИЕ ОБ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Пл-8.5.3-МИДиС-02
Дата введения 01 сентября 2022 г.

Челябинск 2022

Положение об обработке персональных данных рассмотрено и рекомендовано к внедрению решением ученого совета ЧОУВО МИДиС протокол № 01 от 29.08.2022

Разработчики:

Начальник ОТОиСИТ Д.С. Татьянин

26.08.2022
(дата)

Начальник отдела менеджмента качества Л.А. Пашкова

26.08.2022
(дата)

1. Общие положения

1.1. Положение об обработке персональных данных (далее - Положение) определяет условия и порядок обработки персональных данных, которую осуществляет ЧОУВО МИДиС (далее - Оператор).

1.2. Положение разработано во исполнение Политики в отношении обработки персональных данных (далее - Политика) и в соответствии с п. 2 ч. 1 ст. 18.1 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее - ФЗ «О персональных данных»), а также следующими нормативными правовыми актами:

- часть вторая Гражданского Кодекса Российской Федерации от 26 января 1996 г. № 14-ФЗ (далее - часть вторая ГК РФ);
- Трудовой Кодекс Российской Федерации от 30 декабря 2001 г. № 197-ФЗ (далее – ТК РФ);
- часть первая Налогового Кодекса Российской Федерации от 31 июля 1998 г. № 146 ФЗ (далее - часть первая НК РФ);
- Федеральный закон «О бухгалтерском учете» от 6 декабря 2011 г. № 402-ФЗ (далее - ФЗ «О бухгалтерском учете»);
- постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- постановление Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

2. Организация обработки персональных данных

2.1. В целях обеспечения выполнения обязанностей, предусмотренных ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, Оператором назначается ответственный за организацию обработки персональных данных.

2.2. Ответственный за организацию обработки персональных данных обязан:

- организовывать работу Оператора по разработке и принятию организационно-распорядительных документов, регламентирующих деятельность по обработке и защите персональных данных, поддержанию их в актуальном состоянии;
- организовывать принятие Оператором правовых, организационных и технических мер для защиты персональных данных;
- актуализировать перечень работников, имеющих доступ к обработке персональных данных в информационных системах.
- актуализировать перечень работников, допущенных в помещения, в которых осуществляется обработка персональных данных.
- доводить до сведения работников положения законодательства РФ о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;
- публиковать или иным образом обеспечивать неограниченный доступ к документу, определяющему его политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных.
- контролировать процесс ознакомления работников с локальными нормативными актами оператора и законодательством РФ в области защиты персональных данных;

- осуществлять внутренний контроль выполнения Оператором и работниками положений законодательства РФ о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;
- инициировать проведение служебных расследований по фактам нарушения установленных правил обработки и защиты персональных данных;
- направлять в Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций уведомление об обработке персональных данных и информационное письмо о внесении изменений в реестр операторов при необходимости;
- организовывать прием и обработку обращений субъектов персональных данных;
- контролировать заполнение «Журнала учета обращений субъектов персональных данных»;
- проводить оценку эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы Оператора;
- проводить ежегодную оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения ФЗ «О персональных данных»;
- осуществлять допуск работников к персональным данным, обрабатываемым в информационной системе Оператора, а также к их материальным носителям только для выполнения трудовых обязанностей;
- представлять интересы Оператора при проверках надзорных органов в сфере обработки персональных данных.

3. Обеспечение безопасности персональных данных

3.1. Работники, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять их без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

3.2. В целях защиты персональных данных от неправомерных действий (в частности, неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, предоставления, распространения) Оператором применяется комплекс правовых, организационных и технических мер по обеспечению безопасности персональных данных, составляющий систему защиты персональных данных.

3.3. Применение комплекса мер по обеспечению безопасности персональных данных обеспечивает установленный уровень защищенности персональных данных при их обработке в информационной системе Оператора.

3.4. В целях обеспечения выполнения обязанностей, предусмотренных ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, Оператором назначается ответственный за обеспечение безопасности персональных данных в информационных системах.

3.5. Ответственный за обеспечение безопасности персональных данных в информационных системах обязан:

- управлять доступом пользователей в информационной системе;
- управлять полномочиями пользователей в информационной системе;
- поддерживать установленные правила разграничения доступа в информационной системе;
- управлять (администрировать) системой защиты информации (далее – СиЗИ) информационных систем (далее – ИС):

- управлять средствами защиты информации (далее – СЗИ) в ИС;
- управлять программным обеспечением СЗИ;
- восстанавливать работоспособность СЗИ;
- устанавливать обновления программного обеспечения СЗИ, выпускаемых разработчиками (производителями) СЗИ;
- анализировать события в ИС, связанные с защитой информации (события безопасности);
- информировать пользователей об угрозах безопасности информации;
- информировать пользователей о правилах эксплуатации СЗИ;
- обучать пользователей работе со СЗИ;
- управлять доступом к съемным машинным носителям информации, используемым в ИС (определять должностных лиц, имеющих доступ к съемным машинным носителям информации);
- сопровождать функционирование СиЗИ в ходе ее эксплуатации;
- поддерживать конфигурацию СиЗИ (структуру СиЗИ, состав, места установки и параметры настройки СЗИ, программного обеспечения и технических средств) в соответствии с эксплуатационной документацией на СиЗИ (поддержание базовой конфигурации СиЗИ);
- определять лица, которым разрешены действия по внесению изменений в базовую конфигурацию СиЗИ;
- управлять изменениями базовой конфигурации СиЗИ, в том числе: определять типы возможных изменений; разрешать или отказывать во внесении изменений; документировать действия по внесению изменений; хранить данные об изменениях; поддерживать конфигурацию ИС (структуру ИС, состав, места установки и параметры программного обеспечения и технических средств) в соответствии с эксплуатационной документацией на ИС.

- анализировать потенциальные воздействия планируемых изменений в базовой конфигурации СиЗИ на обеспечение защиты информации, возникновение дополнительных угроз безопасности информации и работоспособность ИС.
- определять параметры настройки программного обеспечения, включая программное обеспечение СЗИ, состава и конфигурации технических средств и программного обеспечения до внесения изменений в базовую конфигурацию ИС и СиЗИ.
- выявлять инциденты (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования ИС и (или) к возникновению угроз безопасности информации (далее по тексту – инциденты), и реагирует на них;
- обнаруживать и идентифицировать инциденты, в том числе:

- отказы в обслуживании;
- сбои (перезагрузки) в работе СЗИ;
- нарушения правил разграничения доступа;
- неправомерные действия по сбору информации;
- иные события, приводящие к возникновению инцидентов.

- анализировать инциденты, в том числе определять источники и причины возникновения инцидентов, а также оценивать их последствия;
- планировать меры по устранению инцидентов, в том числе:

- по восстановлению ИС и ее сегментов в случае отказа в обслуживании или после сбоев;

- устранению последствий нарушения правил разграничения доступа, неправомерных действий по сбору информации, внедрения вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;

- планировать и принимать меры по предотвращению повторного возникновения инцидентов;
- контролировать обеспечение класса защищенности ИС:

- контролировать события безопасности и действия пользователей в ИС;

- контролировать (анализировать) защищенность информации, содержащейся в ИС;

- контролировать перемещение съемных машинных носителей информации за пределы контролируемой зоны лицами, которым оно необходимо для выполнения своих должностных обязанностей (функции);

- анализировать и оценивать функционирование СиЗИ ИС, включая выявление, анализ и устранение недостатков в функционировании системы защиты информации ИС;

- выполнять периодический анализ изменения угроз безопасности информации в ИС, возникающих в ходе ее эксплуатации, и принятие мер защиты информации в случае возникновения новых угроз безопасности информации;

- документировать процедуры и результаты контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в ИС;

- принимать решения по результатам контроля (мониторинга) за обеспечением уровня защищенности информации о доработке (модернизации) СиЗИ ИС;

- вести учет:

- используемых шифровальных (криптографических) средств защиты информации в ИС, эксплуатационной и технической документации к ним;

- съемных машинных носителей, используемых в ИС для хранения и обработки информации;

- обеспечивать защиту информации при выводе из эксплуатации ИС или после принятия решения об окончании обработки информации:

- обеспечивать архивирование информации, содержащейся в ИС (архивирование должно осуществляться при необходимости дальнейшего использования информации в деятельности оператора);

- обеспечивать уничтожение (стирание) данных и остаточной информации со съемных машинных носителей информации, при необходимости передачи съемного машинного носителя информации другому пользователю ИС или в сторонние организации для ремонта, технического обслуживания или дальнейшего уничтожения;

- при выводе из эксплуатации съемных машинных носителей информации, на которых осуществлялись хранение и обработка информации, осуществляет физическое уничтожение этих съемных машинных носителей информации.

4. Осуществление прав субъектов персональных данных

4.1. При поступлении обращения субъекта или его представителя, Оператор предоставляет безвозмездно информацию о персональных данных субъекта, а также предоставить возможность ознакомления с этими персональными данными в течение 10 рабочих дней с даты получения запроса субъекта персональных данных или его представителя. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления оператором в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

4.2. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных. В случае отзыва субъектом персональных данных согласия на обработку персональных данных оператор вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 ФЗ «О персональных данных».

4.3. Обязанность предоставить доказательство получения согласия субъекта персональных данных на обработку его персональных данных или доказательство наличия оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 ФЗ «О персональных данных», возлагается на оператора.

4.4. В случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта персональных данных или его представителя оператор обязан дать в письменной форме мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 ФЗ «О персональных данных» или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий десяти рабочих дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления оператором в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

4.5. Оператор обязан предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных. В срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, оператор обязан внести в них необходимые изменения.

4.6. В срок, не превышающий семи рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, оператор обязан уничтожить такие персональные данные. Оператор обязан уведомить субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

4.7. При отсутствии сведений, подтверждающих, что персональные данные субъекта являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, Оператор отказывается вносить изменения и дает ответ субъекту персональных данных.

4.8. Оператор обязан сообщить в уполномоченный орган по защите прав субъектов персональных данных по запросу этого органа необходимую информацию в течение десяти рабочих дней с даты получения такого запроса. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления оператором в адрес уполномоченного органа по защите прав субъектов персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

5. Взаимодействие с Роскомнадзором

5.1. По запросу Роскомнадзора Ответственный за организацию обработки персональных данных организует предоставление локальных нормативных актов в отношении обработки персональных данных и документов, подтверждающих принятие мер по выполнению требований ФЗ «О персональных данных», в течение 10 дней с даты получения запроса. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления оператором в адрес уполномоченного органа по защите прав субъектов персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

5.2. В случае выявления неточных персональных данных по запросу Роскомнадзора Оператор осуществляет блокирование персональных данных, относящихся к этому субъекту персональных данных, с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

5.3. В случае подтверждения факта неточности персональных данных Оператор на основании сведений, представленных Роскомнадзором, или иных необходимых документов уточняет персональные данные в течение семи рабочих дней со дня представления таких сведений и снимает блокирование персональных данных.

5.4. В случае выявления неправомерной обработки персональных данных при запросе Роскомнадзора Оператор осуществляет блокирование неправомерно обрабатываемых персональных данных, относящихся к субъекту персональных данных, с момента получения запроса.

5.5. При выявлении Оператором, Роскомнадзором или иным заинтересованным лицом факта неправомерной или случайной передачи (предоставления, распространения) персональных данных (доступа к персональным данным), повлекшей нарушение прав субъектов персональных данных, Оператор:

- в течение 24 часов - уведомляет Роскомнадзор о произошедшем инциденте, предполагаемых причинах, повлекших нарушение прав субъектов персональных данных, предполагаемом вреде, нанесенном правам субъектов персональных данных, и принятых мерах по устранению последствий инцидента, а также предоставляет сведения о лице, уполномоченном Оператором на взаимодействие с Роскомнадзором по вопросам, связанным с инцидентом;
- в течение 72 часов - уведомляет Роскомнадзор о результатах внутреннего расследования выявленного инцидента и предоставляет сведения о лицах, действия которых стали его причиной (при наличии).

5.6. В случае необходимости Ответственный за организацию обработки персональных данных направляет в Роскомнадзор обращения по вопросам обработки персональных данных, осуществляемой Оператором.

6. Ответственность за нарушение порядка обработки и обеспечения безопасности персональных данных

6.1. В случае нарушения работником положений законодательства в области персональных данных он может быть привлечен к дисциплинарной, материальной, гражданско-правовой, административной и уголовной ответственности в порядке, установленном ТК РФ и иными

федеральными законами, в соответствии с ч. 1 ст. 24 ФЗ «О персональных данных» и ст. 90 ТК РФ.

6.2. В случае разглашения работником персональных данных, ставших ему известными в связи с исполнением его трудовых обязанностей, трудовой договор с ним может быть расторгнут в соответствии с пп. «в» п. 6 ст. 81 ТК РФ.

6.3. Моральный вред, причиненный работнику вследствие нарушения его прав, нарушения правил обработки персональных данных, а также несоблюдения требований к защите персональных данных, установленных Федеральным законом от 27.07.2006 N 152-ФЗ, подлежит возмещению в соответствии с законодательством РФ. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных работником убытков.

Согласовано:

Проректор по учебно-проектной работе

_____Н.А. Попова

29.08.2022

(дата)

Начальник отдела кадров

_____Т.Г. Зыкова

29.08.2022

(дата)

Ответственный секретарь приемной комиссии

_____С.А. Кокорин

29.08.2022

(дата)

Начальник юридического отдела

_____А.А. Аполовников

29.08.2022

(дата)

Приложение 1

Разъяснение юридических последствий отказа предоставить персональные данные

Мне, _____,
(фамилия, имя, отчество)
в соответствии с ч. 2 ст. 18 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» разъяснены юридические последствия моего отказа предоставить свои персональные данные в ЧОУВО МИДиС.
Я предупрежден(а), что без предоставления моих персональных данных в ЧОУВО МИДиС, обязательных для заключения трудового договора согласно ст. 57 и 65 Трудового кодекса Российской Федерации, трудовой договор не может быть заключен.
Мне известно, что на основании п. 11 ч. 1 ст. 77 Трудового кодекса Российской Федерации трудовой договор прекращается вследствие нарушения установленных обязательных правил его заключения, если это нарушение исключает возможность продолжения работы.

«___» _____ 20__г. _____ _____
(подпись) (Ф.И.О.)