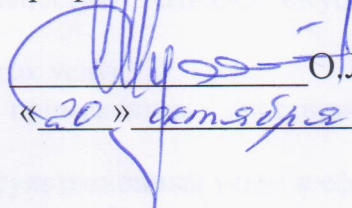


АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ПРОФЕССИОНАЛЬНАЯ
ОБРАЗОВАТЕЛЬНАЯ ОРГАНИЗАЦИЯ
«КУБАНСКИЙ ИНСТИТУТ ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ»
(АНПО «КУБАНСКИЙ ИПО»)

«УТВЕРЖДАЮ»

Директор
автономной некоммерческой
профессиональной образовательной
организации «Кубанский институт
профессионального образования»


О.Л. Шутенко
«20» сентября 2017 года



ПОЛИТИКА

в области обработки и защиты персональных данных
работников и обучающихся

Краснодар, 2017

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая политика в отношении обработки персональных данных (далее – Политика) разработана на основании Конституции РФ, Гражданского кодекса РФ, Трудового кодекса РФ и в соответствии с требованиями федерального закона от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», федерального закона от 27.07.2006 года № 152-ФЗ «О персональных данных», постановления Правительства РФ от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», постановления Правительства РФ от 15.09.2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» и иными законодательными актами, регулирующими деятельность, связанную с персональными данными.

1.2. Цель настоящей Политики – обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных и принятие мер от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных субъектов.

1.3. Персональные данные могут обрабатываться только для целей, непосредственно связанных с деятельностью АНПОО «Кубанский ИПО» (далее – Оператор), в частности для:

- а) предоставления образовательных услуг;
- б) организации обучения с применением дистанционных образовательных технологий;
- в) оказание информационно-консультационных услуг в сфере образования;
- г) принятия решения поступающим на обучение;
- д) проведения семинаров, тренингов и конкурсов;
- е) ведения сайта образовательной организации;
- ж) автоматизации работы библиотеки;
- з) проведения мониторинга деятельности образовательной организации;
- и) трудовых (и других договорных) отношений;
- к) осуществления отбора кандидатов на работу.

1.4. Оператор собирает данные только в объеме, необходимом для достижения вышеназванных целей.

1.5. Передача третьим лицам персональных данных без письменного согласия не допускается. Режим конфиденциальности персональных данных снимается в случаях обезличивания или включения их в общедоступные источники персональных данных, если иное не определено законом.

1.6. Сотрудники, в обязанность которых входит обработка персональных данных субъекта, обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом, а также настоящей Политикой.

1.7. Персональные данные не могут быть использованы в целях причинения имущественного и морального вреда гражданам, затруднения реализации прав и свобод граждан Российской Федерации.

1.8. Лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима обработки и порядка использования этой информации.

1.9. Настоящая политика утверждается директором АНПОО «Кубанский ИПО» и является обязательной для исполнения всеми сотрудниками, имеющими доступ к персональным данным.

1.10. Оператор имеет право вносить изменения в настоящую Политику. При внесении изменений в заголовке Политики указывается дата последнего обновления редакции. Новая редакция Политики вступает в силу с момента ее подписания и размещается на сайте.

1.11. Действующая редакция хранится в месте нахождения Оператора по адресу: г. Краснодар, ул. Садовая, д. 218; электронная версия Политики - на сайте по адресу: <http://vkpo.ru>

2. ТЕРМИНЫ И ПРИНЯТЫЕ СОКРАЩЕНИЯ

2.1. **Персональные данные (ПД)** – любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных).

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

Информационная система персональных данных (ИСПД) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Персональные данные, сделанные общедоступными субъектом персональных данных – персональные данные, доступ неограниченного круга лиц к которым предоставлен самим субъектом персональных данных либо по его просьбе.

Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

Оператор – организация, обрабатывающая персональные данные.

3. ПОНЯТИЕ И СОСТАВ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Персональные данные – любая информация, относящаяся прямо или косвенно к определенному физическому лицу (далее – субъекту). К персональным данным субъекта, которые обрабатывает Оператор, относятся:

- 1) Фамилия, имя, отчество (если есть),
- 2) дата рождения;
- 3) тип документа, удостоверяющего личность, когда и кем выдан, адрес регистрации (фактического проживания);
- 4) сведения о предыдущем уровне образования и документе об образовании и (или) документе об образовании и квалификации, его подтверждающем;
- 5) специальность (с указанием условий обучения и формы получения образования; нуждаемость в общежитии; необходимости создания специальных условий при проведении вступительных испытаний в связи с инвалидностью или ограниченными возможностями здоровья).
- 6) Сведения о воинском учете.
- 7) Сведения об ИНН, страховых свидетельствах государственного пенсионного и медицинского страхования.

- 8) Фотографии для личного дела, студенческого билета и зачетной книжки, снимки общественных мероприятий, размещенных на сайте Оператора.
- 9) Сведения о группе инвалидности.
- 10) Сведения о виде нарушения (нарушений) здоровья.
- 11) Рекомендации, данные по результатам комплексного психолого-медико-педагогического обследования или по результатам медико-социальной экспертизы.
- 12) Информация о смене фамилии, имени, отчества.
- 13) Семейное положение.
- 14) Состав семьи.
- 15) Форма обучения, специальность, номер группы в Институте.
- 16) Данные по успеваемости и выполнению учебного плана.
- 17) Данные о договоре (дополнениям к нему) на получение образовательных услуг.
- 18) Данные по выданным документам о полученном в Институте образовании.
- 19) Данные о трудоустройстве.
- 20) Сведения о поощрениях и наложенных дисциплинарных взысканиях.
- 21) Результаты медицинских обследований.
- 22) Администрирование и контроль трафика Интернета.
- 23) Результаты посещения библиотеки Института.

4. УСЛОВИЯ И ОСНОВНЫЕ ПРИНЦИПЫ ОБРАБОТКИ, ПЕРЕДАЧИ И ХРАНЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Оператор ведет обработку персональных данных субъекта с использованием средств автоматизации (автоматизированная обработка) и без использования таких средств (неавтоматизированная обработка).

4.2. Обработка персональных данных должна осуществляться на основе принципов:

- а) законности целей и способов обработки персональных данных и добросовестности;
- б) соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям Оператора;
- в) соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;
- г) достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;
- д) недопустимости объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных;
- е) уничтожения персональных данных после достижения целей обработки или в случае утраты необходимости в их достижении;
- ж) личной ответственности сотрудников организации за сохранность и конфиденциальность персональных данных, а также носителей информации.

4.3. Оператор должен сообщить субъекту о целях, предполагаемых источниках и способах получения персональных данных, характере подлежащих получению персональных данных, перечне действий с персональными данными, сроке, в течение которого действует согласие, и порядке его отзыва, а также о последствиях отказа субъекта дать письменное согласие на их получение.

4.4. Документы, содержащие персональные данные, создаются путем:

- а) копирования оригинальных документов;
- б) внесения сведений в учетные формы;
- в) получения оригиналов необходимых документов (трудовая книжка, аттестат, медицинское заключение, характеристика и т.д.).

4.5. Обработка персональных данных осуществляется:

а) с согласия субъекта персональных данных на обработку его персональных данных;

б) в случаях, когда обработка персональных данных необходима для осуществления и выполнения возложенных законодательством Российской Федерации функций, полномочий и обязанностей;

в) в случаях, когда осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе (далее – персональные данные, сделанные общедоступными субъектами персональных данных).

4.6. Хранение персональных данных у Оператора осуществляется:

В отделении СПО (отдел учебно-методической работы, отдел воспитательной работы, библиотека) – учебные карточки, формуляры читателей, сведения об успеваемости и посещаемости (журналы и ведомости), зачетные книжки, результаты анкетирований, журналы кураторов, электронные библиотечные системы.

Хранение осуществляется в металлических сейфах, шкафах, закрывающихся на замок. К информации, хранящейся на электронных носителях (компьютерах), доступ осуществляется посредством введения пароля.

Доступ к персональным данным имеют заведующий отделением, ведущие специалисты, преподаватели отделения СПО и другие специалисты в рамках своей компетенции.

В отделении ДПО (учебно-методический центр ДПО, кафедры, центр маркетинга, центр продвижения образовательных программ, центр работы с государственными контрактами) – личные дела слушателей, ведомости учета успеваемости, журналы учета посещаемости, приказы о движении контингента, списки слушателей, протоколы заседаний аттестационных комиссии, акты выполненных работ, бланки строгой отчетности.

Хранение осуществляется в металлических сейфах, шкафах, закрывающихся на замок. К информации, хранящейся на электронных носителях (компьютерах), доступ осуществляется посредством введения пароля.

Доступ к ПД имеют руководители центров, заведующие кафедрами, ведущие специалисты, преподаватели в рамках своей компетенции.

В Приемной комиссии (отдел правового и кадрового обеспечения, бухгалтерия, медкабинет, отдел ТЭО) – личные дела поступающих, личные дела студентов, личные дела сотрудников, трудовые книжки, личные медицинские книжки, электронная база ФИС ФРДО (приемная комиссия и дипломы), работа с центром занятости, оригиналы документов об образовании, сайт Оператора.

Хранение осуществляется в металлических сейфах, шкафах, закрывающихся на замок. К информации, хранящейся на электронных носителях (компьютерах), доступ осуществляется посредством введения пароля или с использованием электронной цифровой подписи в том числе.

Доступ к персональным данным имеют руководители отделов, ведущие специалисты и иные сотрудники в рамках своей компетенции.

4.5. Сотрудникам, допущенным к обработке персональных данных, запрещается:

При работе с документами, содержащими персональные данные, сотрудники обязаны исключить возможность ознакомления, просмотра этих документов лицами, не допущенными к работе с ними (в том числе другими работниками).

Делать неучтенные копии документов, содержащие персональные данные.

Оставлять документы, содержащие персональные данные, на рабочих столах без присмотра.

Покидать помещение, не поместив документы с персональными данными в закрываемые сейфы, шкафы (как в течение рабочего дня, так и в конце рабочего дня).

Разглашать информацию, полученную в процессе ознакомления с персональными данными работников и/или обучающихся.

Пересылать с рабочей электронной почты на личную электронную почту или почту третьего лица без письменного согласия (разрешения, приказа, распоряжения) Работодателя информацию, отнесенную к коммерческой или иной охраняемой законом тайне (конфиденциальная информация, в том числе персональные данные), которая стала известна при исполнении работником трудовой функции.

Выносить документы, содержащие персональные данные, из помещений организации без служебной необходимости.

5. СВЕДЕНИЯ О ТРЕТЬИХ ЛИЦАХ, УЧАСТВУЮЩИХ В ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. В целях соблюдения законодательства РФ, для достижения целей обработки, а также в интересах и с согласия субъектов персональных данных Оператор в ходе своей деятельности предоставляет персональные данные следующим организациям:

- а) Министерству образования, науки и молодежной политики Краснодарского края (Министерству образования и науки РФ);
- б) Федеральной налоговой службе РФ;
- в) Пенсионному фонду России;
- г) Фонду социального страхования РФ;
- д) Федеральной службе государственной статистики РФ;
- е) Фонду обязательного медицинского страхования РФ;
- ж) Банкам для начисления заработной платы (на основании договора);
- з) Правоохранительным органам (в случаях, установленных законодательством);
- и) Кредитным организациям (с согласия субъекта);
- к) Лицензирующим и/или контролирующим органам государственной власти и местного самоуправления.

5.2. Оператор не поручает обработку персональных данных другим лицам на основании договора.

6. ОБЯЗАННОСТИ ОРГАНИЗАЦИИ-ОПЕРАТОРА

6.1. В целях обеспечения прав и свобод человека и гражданина организация при обработке персональных данных субъекта обязана соблюдать следующие общие требования:

а) обработка персональных данных субъекта может осуществляться исключительно в целях оказания законных услуг физическим и юридическим лицам;

б) персональные данные субъекта следует получать у него самого. Если персональные данные субъекта возможно получать только у третьей стороны, то субъект должен быть уведомлен об этом заранее, и от него должно быть получено письменное согласие. Оператор должен сообщить субъекту о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа субъекта дать письменное согласие на их получение;

в) оператор не имеет права получать и обрабатывать персональные данные, относящиеся к специальным категориям персональных данных (о расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, интимной жизни). Обработка указанной выше информации допускается в ситуациях, предусмотренных законом:

- только с письменного согласия субъекта;

- если обработка персональных данных осуществляется в соответствии с законодательством о государственной социальной помощи, трудовым законодательством, пенсионным законодательством РФ.

г) предоставлять субъекту или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с ними при обращении субъекта персональных данных или его представителя либо в течение 30 дней с даты получения запроса субъекта персональных данных или его представителя;

д) хранение и защита персональных данных субъекта от неправомерного их использования или утраты обеспечивается оператором безвозмездно, в порядке, установленном действующим законодательством РФ;

е) в случае выявления недостоверных персональных данных или неправомерных действий с ними оператора при обращении по запросу субъекта либо уполномоченного органа по защите прав субъектов персональных данных, оператор обязан осуществить блокирование персональных данных на период проверки;

ж) в случае подтверждения факта недостоверности персональных данных, оператор на основании документов, предоставленных субъектом либо уполномоченным органом по защите прав субъектов персональных данных или иных необходимых документов обязан уточнить персональные данные и снять с них блокирование;

з) в случае достижения цели обработки персональных данных организация обязана незамедлительно прекратить обработку персональных данных и уничтожить соответствующие персональные данные в срок, не превышающий 3-х рабочих дней, и уведомить об этом субъект, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, также в указанный орган;

и) в случае отзыва субъектом согласия на обработку своих персональных данных, оператор обязан прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий трех рабочих дней, если иное не предусмотрено соглашением между организацией и субъектом. Об уничтожении персональных данных организация обязана уведомить субъекта.

7. ПРАВА СУБЪЕКТА

7.1. Право на доступ информации о самом себе.

7.2. Право на отзыв согласия на обработку персональных данных.

7.3. Право требовать от оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки.

7.4. Право обжаловать неправомерные действия или бездействия по обработке персональных данных и требовать соответствующей компенсации в суде.

7.5. Право на дополнение персональных данных оценочного характера заявлением, выражающим его собственную точку зрения.

7.6. Право определять представителей для защиты своих персональных данных.

7.7. Право требовать от организации уведомления всех лиц, которым ранее были сообщены неверные или неполные персональные данные субъекта, обо всех произведенных в них изменениях или исключениях из них.

8. ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ СУБЪЕКТА

8.1. Персональные данные субъекта могут быть предоставлены третьим лицам только с письменного согласия субъекта.

8.2. Доступ субъекта к своим персональным данным предоставляется при обращении либо при получении запроса субъекта. Оператор обязан сообщить информацию о наличии персональных данных о нем, а также предоставить возможность ознакомления с ними в течение 30 рабочих дней с момента обращения или получения запроса.

8.3. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись субъекта персональных данных или его законного представителя. Запрос может быть направлен в электронной форме и подписан электронной цифровой подписью в соответствии с законодательством РФ.

8.4. Субъект имеет право на получение при обращении или при отправлении запроса информации, касающейся обработки его персональных данных, в том числе содержащей:

- а) подтверждение факта обработки персональных данных оператором, а также цель такой обработки;
- б) способы обработки персональных данных, применяемые организацией;
- в) сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;
- г) перечень обрабатываемых персональных данных и источник их получения;
- д) сроки обработки персональных данных, в том числе срок их хранения;
- е) сведения о том, какие юридические последствия для субъекта может повлечь за собой обработка его персональных данных.

8.5. Сведения о наличии персональных данных должны быть предоставлены субъекту в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных.

8.6. Право субъекта на доступ к своим персональным данным ограничивается в случае, если предоставление персональных данных нарушает права и законные интересы третьих лиц.

9. МЕРЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

9.1. Под угрозой или опасностью утраты персональных данных понимается единоличное или комплексное, реальное или потенциальное, активное или пассивное проявление злоумышленных возможностей внешних или внутренних источников угрозы создавать неблагоприятные события, оказывать дестабилизирующее воздействие на защищаемую информацию.

9.2. Риск угрозы любым информационным ресурсам создают стихийные бедствия, экстремальные ситуации, террористические действия, аварии технических средств и линий связи, другие объективные обстоятельства, а также заинтересованные и незаинтересованные в возникновении угрозы лица.

9.3. Защита персональных данных представляет собой жестко регламентированный технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и, в конечном счете, обеспечивающий достаточно надежную безопасность информации в процессе деятельности оператора.

9.4. В соответствии с требованиями нормативных документов Оператором создана система защиты персональных данных (СЗПД), состоящая из подсистем правовой, организационной и технической защиты.

9.5. Подсистема правовой защиты представляет собой комплекс правовых, организационно-распорядительных и нормативных документов, обеспечивающих создание, функционирование и совершенствование системы защиты персональных данных.

9.6. Подсистема организационной защиты включает в себя организацию структуры управления системы защиты персональных данных, разрешительной системы, защиты информации при работе с сотрудниками, партнерами и сторонними лицами, защиты

информации в открытой печати, публицистической и рекламной деятельности, аналитической работе.

9.7. Подсистема технической защиты включает в себя комплекс технических, программных, программно-аппаратных средств, обеспечивающих защиту персональных данных.

9.8. Основными мерами защиты персональных данных, используемыми Оператором, являются:

- а) назначение лица, ответственного за обработку персональных данных, которое осуществляет организацию обработки персональных данных, обучение и инструктаж, внутренний контроль за соблюдением Оператором и его работниками требований к защите персональных данных;
- б) определение актуальных угроз безопасности персональных данных при их обработке, и разработка мер и мероприятий по защите персональных данных;
- в) разработка политики в отношении обработки персональных данных и Положения о защите персональных данных;
- г) установление правил доступа к персональным данным, а также обеспечения регистрации и учета всех действий, совершаемых с персональными данными;
- д) установление индивидуальных паролей доступа сотрудников в информационную систему в соответствии с их производственными обязанностями;
- е) применение прошедших в установленном порядке процедур оценки соответствия средств защиты информации;
- ж) сертифицированное программное средство защиты информации от несанкционированного доступа;
- з) сертифицированное антивирусное программное обеспечение с регулярно обновляемыми базами;
- и) сертифицированные межсетевой экран и средство обнаружения вторжения;
- к) соблюдение условий, обеспечивающих сохранность персональных данных и исключающих несанкционированный к ним доступ;
- л) обнаружение фактов несанкционированного доступа к персональным данным и принятия необходимых мер;
- м) восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- н) обучение работников Оператора, непосредственно осуществляющих обработку персональных данных, положениям законодательства РФ о персональных данных, в том числе требованиям к защите персональных данных, ознакомление с документами, определяющими политику Оператора в отношении обработки персональных данных, с локальными актами по вопросам обработки персональных данных;
- о) осуществление внутреннего контроля и аудита.

10. ОТВЕТСТВЕННОСТЬ ЗА РАЗГЛАШЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

10.1. Оператор несет ответственность за персональную информацию, которая находится в его распоряжении и закрепляет персональную ответственность сотрудников за соблюдением конфиденциальности информации ограниченного доступа.

10.2. Каждый сотрудник организации, получающий для работы доступ к материальным носителям персональных данных, несет ответственность за сохранность носителя и конфиденциальность информации.

10.3. Любое лицо может обратиться к сотруднику организации с жалобой на нарушение данной Политики. Жалобы и заявления по поводу соблюдения требований обработки данных рассматриваются в течение 30-ти рабочих дней с момента поступления.

10.4. Сотрудники организации обязаны на должном уровне обеспечивать рассмотрение запросов и жалоб субъектов, а также содействовать исполнению требований компетентных органов. Лица, виновные в нарушении требований настоящей Политики,

привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Трудовым Кодексом РФ и иными федеральными законами, а также к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.