Приложение 1

УТВЕРЖДАЮ
Директор Слободского колледжа
педагогики и социальных отношений
_____ О.М. Шеренцова
«____» _____ 20___ г.

КИРОВСКОЕ ОБЛАСТНОЕ ГОСУДАРСТВЕННОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ " СЛОБОДСКОЙ КОЛЛЕДЖ ПЕДАГОГИКИ И СОЦИАЛЬНЫХ ОТНОШЕНИЙ"

Подписан: КИРОВСКОЕ ОБЛАСТНОЕ ГОСУДАРСТВЕННОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ " СЛОБОДСКОЙ КОЛЛЕДЖ ПЕДАГОГИКИ И СОЦИАЛЬНЫХ ОТНОШЕНИЙ"
DN: C=RU, S=Кировская область, STREET="Кировская область, город Слободской, улица Рождественская 69", L=г. Слободской, T=Директор, O="КИРОВСКОЕ ОБЛАСТНОЕ ГОСУДАРСТВЕННОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ ""СЛОБОДСКОЙ КОЛЛЕДЖ ПЕДАГОГИКИ И СОЦИАЛЬНЫХ ОТНОШЕНИЙ""", ОГРН=1024301078680, СНИЛС=05905745986, OID.1.2.643.100.4=4343002804, ИНН=432900689860, E=slbux@mail.ru, G=Ольга Михайловна, SN=Шеренцова, CN="КИРОВСКОЕ ОБЛАСТНОЕ ГОСУДАРСТВЕННОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ ""СЛОБОДСКОЙ КОЛЛЕДЖ ПЕДАГОГИКИ И СОЦИАЛЬНЫХ ОТНОШЕНИЙ"""
Основание: я подтверждаю этот документ своей удостоверяющей подписью

Положение
по обработке и защите персональных данных

Слободской , 2018

Содержание

1. Общие сведения

1.1. Назначение документа

Настоящий документ устанавливает порядок организации обработки персональных данных в КОГПОБУ СКПиСО (далее - Оператор), а именно порядок получения, учета, обработки, накопления и хранения документов, содержащих сведения, отнесенные к персональным данным работников Оператора и контингента обучающихся.

Порядок разработан в соответствии с требованиями действующего законодательства Российской Федерации о защите персональных данных.

Общие сведения о правовых основаниях, категориях субъектов персональных данных и целях обработки персональных данных определены в Политике КОГПОБУ СКПиСО в отношении обработки персональных данных.

1.2. Область применения

Область применения настоящего Положения определяется Политикой КОГПОБУ СКПиСО в отношении обработки персональных данных, утвержденной приказом.

1.3. Аудитория

Порядок предназначен для служебного пользования сотрудниками Оператора, в обязанности которых входит:

- организация обработки персональных данных;
- обработка персональных данных;
- обеспечение защиты персональных данных.

2. Организация обработки персональных данных

2.1. Цель организации обработки персональных данных

Целью организации обработки персональных данных является достижение уверенности руководства Оператора в том, что права субъектов персональных данных защищаются организацией в соответствии с законодательством РФ.

Цель Положения – защита персональных данных работников и контингента обучающихся от несанкционированного доступа и разглашения.

2.2. Сферы ответственности

Для достижения конфиденциальности обработки персональных данных оформлены следующие сферы ответственности:

- организация обработки персональных данных;
- организация физической безопасности и охраны объектов;
- информационные технологии;
- информационная безопасность.

В отношении каждой сферы ответственности приказом явным образом должно быть назначено ответственное лицо.

2.3. Установление и пересмотр требований к обработке персональных данных

Требования к обработке персональных данных устанавливаются для каждого вида деятельности в форме внутренних организационно-распорядительных документов.

Установленные требования подлежат пересмотру 1 раз в год либо чаще при существенном изменении условий обработки и (или) требований к защите персональных данных.

2.4. Контроль условий обработки ПДн

В целях поддержания уровня защищенности прав субъектов персональных данных и соответствия выполняемых мероприятий внутренним и внешним требованиям выполняется периодический контроль соответствия, не реже 1 раза в год.

Результаты контроля оформляются в форме Отчета, который разрабатывается ответственным за организацию обработки персональных данных и согласовывается с ответственными лицами и утверждается директором.

В Отчете рассматриваются следующие вопросы:

- условия обработки персональных данных;
- описание процессов обработки персональных данных;
- перечень персональных данных;
- перечень информационных систем персональных данных и их оценка;
- режимные мероприятия;
- организация обработки персональных данных;
- перечень существующих документов, регулирующих обработку и обеспечивающих безопасность персональных данных;
- защита персональных данных;
- контроль объема и сроков обработки персональных данных как в автоматизированной форме, так и неавтоматизированной (избыточные по срокам и объёмам данные либо обезличиваются либо уничтожаются);
- заключение о соответствии и эффективности мероприятий;
- решения по улучшении системы организации обработки персональных данных.

2.5. Ключевые требования к сотрудникам и обратной связи

Сотрудники, на которых возложены обязанности по обработке и организации защиты персональных данных, должны:

- уметь отличать персональные данные от другой информации и уважать интересы их владельца;
- соблюдать условия обработки персональных данных (цели, сроки, объемы и основания);
- отличать ситуации, в которых основания для обработки персональных данных отсутствуют, не осуществлять обработку, если на то нет оснований;
- защищать персональные данные в соответствии с установленными мерами защиты.

2.6. Ограничение и контроль доступа к персональным данным

Доступ к персональным данным ограничивается:

- должностными инструкциями;
- приказом о допуске к обработке ПДн;
- приказом о допуске в помещения.

Организацию допуска осуществляет лицо, ответственное за организацию обработки персональных данных.

Сотрудник, допущенный к обработке персональных данных:

- обязан подписать обязательство о неразглашении персональных данных (Приложение №2)

– имеет право получать только те сведения о субъекте, которые необходимы ему для выполнения конкретных функций в соответствии с его должностными обязанностями;

– должен быть компетентен по вопросам обработки персональных данных;

– имеет право обрабатывать ПДн в рамках своих обязанностей на персональном компьютере при условии выполнения мер по защите информации на его рабочем месте;

– при изменении полномочий или увольнении должен прекратить обработку ПДн, вернуть все имеющиеся документы с персональными данными в соответствующее подразделение, уничтожить файлы, содержащие ПДн.;

– несет ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты персональных данных.

Уровень компетентности сотрудников в части обработки персональных данных обеспечивается ответственным за организацию обработки персональных данных, а также непосредственными руководителями сотрудников.

2.7. Контроль изменения в статусе и условиях работы сотрудников

При всех изменениях в должностных обязанностях, месте и характере работы сотрудников, допущенных к обработке персональных данных следует руководствоваться следующими правилами:

– все изменения, существенным образом влияющие на должностные обязанности и на уровень доступа к персональным данным должны контролироваться специалистом по кадровой работе;

– специалист по кадровой работе информирует ответственных лиц о произошедших изменениях;

– при приёме на работу, увольнении или переводе сотрудника выполняется обход ответственных лиц, которые должны принять меры по изменению полномочий доступа сотрудников;

– при увольнении или переводе сотрудник должен возвратить ценности, информацию на бумажных и электронных носителях, доступ к которой ему больше не нужен;

– ответственные лица актуализируют меры по ограничению доступа в рамках своей компетенции.

2.8. Ознакомление сотрудников с документами

Сотрудники, допущенные к обработке персональных данных, должны быть ознакомлены с внутренними локальными документами Оператора по вопросам обеспечения безопасности персональных данных под роспись.

Ознакомление может быть:

– первичным, при приеме на работу;

– плановым, при утверждении новых или изменении, дополнении уже существующих внутренних локальных документов.

2.9. Порядок доступа сотрудников в помещения

Организационные меры в области физической безопасности персональных данных должны включать:

– назначение лица, ответственного за кабинет;

– определение помещений с ограниченным доступом и комплекса мер по защите помещений;

– назначение лица, ответственного за контроль средств доступа (ключей от помещений, оконных решеток, шкафов, сейфов, прокси-карточек);
– охранная сигнализация и тревожная кнопка;
– пожарная сигнализация;
– дополнительное ограничение доступа при входе в здание .

2.10. Организация прохождения документов

Документы, содержащие персональные данные, обрабатываются в соответствии с порядками, установленными законодательством, отраслевыми нормативными документами, локальными документами Оператора.

2.11. Меры по защите информации

Оценка угроз безопасности персональных данных и принятие на её базе решений по защите информации проводится Оператором регулярно не реже 1 раза в год. Результат оценки отражается в отчете.

Сотрудник, ответственный за информационную безопасность, обеспечивает необходимый уровень компетентности сотрудников Оператора в части особенностей работы с информационными системами персональных данных, контролирует их допуск к работе на компьютерах только после проведения обучения и инструктажа.

Процедуры обработки персональных данных

3.1. Получение персональных данных

Персональные данные субъекта могут поступить Оператору от самого субъекта либо от третьей стороны.

Независимо от способа получения персональных данных:

1) личность субъекта персональных данных должна быть подтверждена сотрудниками Оператора (по удостоверению личности);
2) правомерность обработки его персональных данных должна быть установлена.

Оператор может получать персональные данные исключительно в объеме, соответствующем целям обработки.

При получении персональных данных от субъекта сотрудник должен проверить их достоверность.

Предоставляя свои персональные данные, субъект должен быть проинформирован об условиях их обработки. Информирование может осуществляться в форме ознакомления с Политикой КОГПОБУ СКПиСО в отношении обработки персональных данных.

От субъекта данные могут быть получены путем:

– получения оригиналов (копий) необходимых документов;
– копирования оригиналов документов;
– внесения сведений в учетные формы;
– в процессе работы с ним.

При необходимости получить персональные данные субъекта от третьей стороны сотрудник, должен уведомить об этом субъекта не позднее 5 дней до даты запроса, сообщив ему о целях, объеме, предполагаемых источниках и способах получения данных, и получить его согласие на запрос сведений.

При поступлении информации о субъекте от отправителя, личность которого не может быть идентифицирована (по электронной почте, факсу и т.п.), сотрудник обязан:

1. При необходимости установления контакта с субъектом и продолжения работы с ним – пригласить его на территорию предприятия и в последствии при контакте выполнить его идентификацию.
2. В отсутствие необходимости продолжения контакта с субъектом – не реагировать и удалить сообщение.

3.2.Отказ субъекта предоставить персональные данные

Если субъект отказывается предоставить сведения, необходимые и обязательные для целей их обработки, установленных законом, договором, то сотрудник, ответственный за сбор сведений, должен разъяснить ему юридические последствия такого отказа (с указанием законодательных оснований).

3.3.Согласие на обработку ПДн и его отзыв

Согласие субъекта на обработку его ПДн необходимо в случаях, в которых обязанность Оператора обрабатывать ПДн необходима, но не предусмотрена законодательством РФ, договором с Субъектом или другими условиями пп2-11 пункта 1 статьи 6 закона РФ №152-ФЗ «О персональных данных».

3.4.Обратная связь с субъектом

Сотрудник Оператора может осуществлять обратную связь с субъектом персональных данных только по тем контактным данным, которые:

– предоставил сам субъект (например, указал в согласии, оставил визитку);

3.5.Подход к оценке вреда субъектам персональных данных

Оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения требований законодательства в области персональных данных устанавливается руководством.

3.6.Конфиденциальность персональных данных

Сотрудники, получившие доступ к персональным данным субъектов, должны соблюдать в их отношении режим конфиденциальности, не раскрывать третьим лицам и не распространять их без наличия соответствующих оснований .

3.7.Идентификация субъекта персональных данных

Субъекты ПДн, а также все сотрудники и лица, обрабатывающие ПДн, должны быть идентифицированы сотрудниками Оператора. Должен быть установлен тот факт, что обрабатываемые персональные данные субъекта принадлежат именно ему и доступ к ним получают только установленные лица. Все такие лица здесь именуются Субъектами.

Идентификация Субъекта может осуществляться с помощью:

– документов, удостоверяющих личность субъекта;

– идентификаторов (в зависимости от рабочего инструментария - логинов, паролей, сертификатов электронной подписи, адресов электронной почты, номеров телефона, средств мгновенных сообщений, бесконтактных карточек доступа в помещения).

Пользователи и ответственные лица обязаны обеспечивать конфиденциальность паролей!

3.8.Передача персональных данных третьим лицам

Оператор передает персональные данные субъекта третьим лицам в случаях:

– если субъект дал свое согласие на передачу данных 3-му лицу;

– обязательной передачи сведений, определенных законодательством Российской Федерации.

Передачу персональных данных осуществляют уполномоченные сотрудники в бумажной или электронной форме в рамках своих полномочий и в объеме, соответствующем целям передачи.

Случаи передачи фиксируются в Журнале регистрации выдачи справок, выписок из документов персональных данных.

3.9.Случаи обязательной передачи персональных данных третьим лицам

Оператор обязан вести обработку и передавать персональные данные субъекта в целях осуществления его прав соответствующим инстанциям. В зависимости от категории субъекта такая передача обязательна в соответствии с законодательством о государственной социальной помощи, трудовым законодательством, законодательством о пенсиях по государственному пенсионному обеспечению и о трудовых пенсиях, об обязательных видах страхования, воинском учете и др.

Также Оператор обязан вести обработку и передавать персональные субъектов в соответствии с законодательством Российской Федерации при поступлении официальных запросов из налоговых органов, судебных органов, правоохранительных органов, судов, организаций, ведущих оперативно-розыскные мероприятия, исполнительное производство и др.

Оператор вправе осуществлять такую передачу без согласия субъекта.

3.10. Трансграничная передача персональных данных

Трансграничная передача персональных данных не осуществляется

3.11. Поручение обработки персональных данных

Поручение обработки персональных данных третьим лицам не осуществляется.

3.12. Подтверждение сведений о субъекте третьей стороне

Оператор может предоставлять субъектам документы (выписки, протоколы, справки и т.п.), которые могут передаваться им третьей стороне, например, банкам, кредитным, туристическим, визовым и другим организациям.

3.13. Неавтоматизированная обработка персональных данных

Порядок обработки персональных в бумажной форме без использования средств автоматизации определен в Инструкции по неавтоматизированной обработке персональных данных.

3.14. Автоматизированная обработка персональных данных

Автоматизированная обработка персональных данных должна осуществляться в объеме, не превышающем объем неавтоматизированной обработки.

3.15. Контроль сроков обработки персональных данных

Руководители подразделений, обрабатывающих персональные данные, периодически (не реже 1 раза в год) должны организовывать проведение контроля. Данное правило касается как автоматизированной так и неавтоматизированной обработки.

3.16. Уничтожение персональных данных

Порядок уничтожения персональных в бумажной форме определен в Инструкции по неавтоматизированной обработке персональных данных.

Персональные данные в электронной форме стираются, желательно с использованием программ надежного удаления данных, либо выводятся из использования путем нанесения необратимого вреда носителю электронной информации.

3.17. Правило «чистого стола»

При отсутствии сотрудника Оператора, использующего персональные данные субъектов, на рабочем месте все документы, содержащие такие данные:

- на бумажном носителе должны быть убраны со стола в ящики, сейф, шкафы или иные места хранения, исключающие бесконтрольный доступ к ним;
- изображение экрана монитора должно быть заблокировано для исключения бесконтрольно просмотра (нажатием «Windows+L»);
- при отсутствии активности сотрудника в течение 30 минут рабочий стол должен блокироваться автоматически.

3.18. Видеонаблюдение в помещениях Оператора

Для обеспечения безопасности в помещениях Оператора может осуществляться видеонаблюдение.

Посетители информируются об этом в форме информационных табличек.

3.19. Работа с обращениями и запросами субъектов

Учет всех обращений и запросов субъекта по вопросам обработки его персональных данных, в том числе отзыв согласия, организуются ответственным за организацию обработки персональных данных. Учет ведется в Журнале учета обращений субъектов персональных данных сотрудниками.

При отказе в удовлетворении обращения или запроса субъекта сотрудник обязан предоставить субъекту мотивированный ответ в письменной форме с указанием правового основания отказа.

3.20. Прекращение обработки персональных данных

При истечении срока обработки персональных данных их обработка должна быть прекращена одним из способов:

- возврат субъекту его персональных данных;
- уничтожение персональных данных.

3.21. Общедоступные ПДн

Обработка общедоступных персональных данных допускается при условии наличия доказательств их получения из общедоступных источников.

В частности, если такие данные получены из социальных сетей, то допускается их обработка только в рамках работы с соответствующей социальной сетью для целей информирования её пользователей об услугах Оператора.

3.22. Обработка обезличенных персональных данных

Обезличенные персональные данные – это данные, по которым невозможно без использования дополнительной информации определить субъекта.

Такие данные могут обрабатываться Оператором без согласия субъектов персональных данных при условии, что Оператором не обладает идентификационной информацией, позволяющей связать эти данные с субъектами ПДн.

Обезличивание персональных данных выполняется для выполнения в дальнейшем статистических расчетов и других задач.

Приложение №1 – Типовая форма разъяснения юридических последствий

ТИПОВАЯ ФОРМА
Разъяснения субъекту юридических последствий отказа предоставить свои персональные данные

Мне,

_____
(фамилия имя отчество)

разъяснены юридические последствия отказа предоставить свои персональные данные в «Наименование организации».

В соответствии с _____
(статьи закона, на основании которых субъект

_____
персональных данных должен предоставить персональные данные)

субъект персональных данных обязан предоставить определенный перечень документов и информации о себе.

Без предоставления субъектом персональных данных обязательных для

_____
(цель предоставления персональных данных)

_____
(последствие отказа непредставления персональных данных)

_____

_____

«_____» _____20__ года _____ _____

Приложение №2 – Обязательство сотрудника о неразглашении персональных данных

Типовое обязательство сотрудника, непосредственно осуществляющего обработку персональных данных, об обеспечении конфиденциальности персональных данных

Я,_____,
(фамилия, имя, отчество)

_____
(должность)

_____,

обязуюсь соблюдать конфиденциальность персональных данных, ставших известными мне в связи с исполнением должностных обязанностей, а также меры, установленные КОГПОБУ СКПиСО по обеспечению безопасности и защиты персональных данных.

В случае расторжения со мной трудового договора добровольно принимаю на себя обязательства:

- прекратить обработку персональных данных, ставших известными мне в связи с исполнением должностных обязанностей;
- не разглашать, не раскрывать сведения, составляющие персональные
- данные субъектов персональных данных;
- не передавать третьим лицам сведения, составляющие персональные данные субъектов персональных данных, которые мне стали известны при исполнении должностных обязанностей;
- вернуть все носители, содержащие персональные данные субъектов персональных данных, которые находились в моем распоряжении в связи с выполнением мною должностных обязанностей.

Я предупрежден (-а) о том, что в случае нарушения требований данного обязательства, буду привлечена к ответственности в соответствии с законодательством Российской Федерации.

_____ _____
(подпись) (расшифровка подписи)

"___" _____ 20___ г.

Приложение №3 – Журнал учета запросов и обращений субъектов персональных данных

Журнал учета обращений Субъектов персональных данных

№ п/п	Дата	Запрашивающее лицо	Состав запрашиваемых данных	Цель запроса	Отметка об удовлетворении запроса либо отказе	Дата удовлетворения или отказа	Причина отказа	Подпись запрашивающего лица	Подпись ответственного сотрудника	Примечание
1	2	3	4	5	6	7	8	9	10	11