ООО «Государство Детей»
ИНН 7718989746 КПП 771701001
ОГРН 1147746809704
тел.: +7 (925) 258-46-47

Перечень организационно-технических мер по защите персональных данных для региональных организаций-пользователей АИС «Навигатор»

Уважаемые коллеги!

Серверный сегмент АИС «Навигатор дополнительного образования детей» (далее АИС «Навигатор») вашего региона прошел аттестацию на соответствие требованиям безопасности информации законодательства РФ. Согласно законодательству РФ, Ваша организация имеет статус оператора персональных данных. В связи с этим направляем Вам перечень обязательных мер по защите персональных данных, которые должны быть реализованы в Вашей организации. По любым вопросам, касающимся реализации перечисленных ниже мер, рекомендуем Вам обращаться в организацию, выполняющую функции администратора АИС «Навигатор» в Вашем регионе.

Обязательные организационно-технические меры по защите персональных данных

В соответствии с Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных» Ваша организация, как оператор персональных данных, обязана принять меры ФЗ 152, и согласно Приказу ФСТЭК России №21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», Ваша организация должна соблюдать следующие меры:

1. Утвердить пакет организационно-распорядительных документов по образцу типового комплекта, прилагаемого Вам в архиве, и ознакомить под подпись с этими документами всех сотрудников организации. Вы также можете получить образцовый комплект документов от организации, выполняющей функции администратора АИС «Навигатор» в Вашем регионе.
2. Обеспечить реализацию на рабочем месте каждого пользователя АИС «Навигатор» следующих технических мер защиты информации:
   2.1. Доступ к учётной записи пользователя должен осуществляться только по паролю.
   2.2. Необходимо, чтобы брандмауэр или любой другой вид межсетевого экрана был включен и настроен для рабочей сети.
   2.3. Права пользователя и администратора должны быть строго разделены. Самостоятельная установка программного обеспечения пользователем должна быть запрещена.
   Реализация мер 2.1, 2.2, 2.3 может быть осуществлена средствами ОС Windows или же установкой на рабочее место сертифицированного СЗИ Secret Net Studio «Постоянная Защита» или сертифицированного эквивалента.
   2.4. Должна быть установлена сертифицированная антивирусная программа, например, медиа-комплект **Web Enterprise Security Suite**.

2.5. Для анализа уязвимостей системы настоятельно рекомендуется использовать программные средства анализа защищенности (САЗ). К сертифицированным САЗ относится программа «Сканер-ВС», к несертифицированным – бесплатная программа от ФСТЭК “ScanOval”.

3. Уведомить в установленном порядке Роскомнадзор о том, что Ваша организация является оператором персональных данных (если такое уведомление не подавалось ранее) или дополнить поданное ранее уведомление новыми сведениями – в соответствии с данными по использованию АИС «Навигатор». Образец уведомления находится в Приложении к данному перечню.

Ответственность за нарушение законодательства РФ в области персональных данных

Напоминаем Вам, что статьёй 13.11 Кодекса Российской Федерации об административных правонарушениях (КоАП РФ) установлена ответственность физических и юридических лиц за нарушения законодательства в области персональных данных, в частности:

- Вторая часть статьи 13.11 КоАП РФ предусматривает ответственность в форме штрафа (для юридических лиц – до 75 000 рублей) за обработку персональных данных без согласия субъекта персональных данных, либо за обработку персональных данных с нарушением требований к составу сведений, включаемых в письменное согласие.
- В соответствии с третьей частью статьи 13.11 КоАП РФ оператору будет вынесено предупреждение или штраф (для юридических лиц – до 30 000 рублей) за невыполнение обязанности по опубликованию или обеспечению иным образом неограниченного доступа к политике оператора в отношении обработки персональных данных, а также при необеспечении доступа к сведениям о реализуемых требованиях к защите персональных данных.

Приложение

Заполнение уведомления об обработке персональных данных в электронном виде

В соответствии со статьей 22 Федерального закона №152-ФЗ «О персональных данных» Оператор до начала обработки персональных данных обязан уведомить уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных. Электронный бланк уведомления можно найти на официальном сайте Роскомнадзора вместе с Методическими рекомендациями по составлению уведомления и образцом заполнения. Приводимый ниже пример заполнения электронного бланка учитывает особенности обработки персональных данных в АИС «Навигатор». Подчеркиваем, что этот пример заполнения НЕ включает в себя информацию о других типах персональных данных, которые могут обрабатываться в Вашей организации для задач, не связанных с использованием АИС «Навигатор».

ООО «Государство Детей»
ИНН 7718989746 КПП 771701001
ОГРН 1147746809704
тел.: +7 (925) 258-46-47

Корректно составленное уведомление должно включать в себя информацию о работе со всеми типами персональных данных, которые обрабатываются в организации.

1	**Тип оператора**	Юридическое лицо
2	**Наименование оператора**	Полное наименование юр. лица Вашей организации
3	**Сокращенное наименование оператора**	
4	**Контактные данные**	В соответствии с данными по Вашей организации
5	**Правовое основание обработки персональных данных**	Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации», письмо министерства образования Ставропольского края в адрес учредителя Вашей организации о работе в АИС «Навигатор»
6	**Цель обработки персональных данных**	Обработка заявок на обучение, учет обучающихся; Инвентаризация, учет загрузки педагогов.

7	**Описание мер, предусмотренных статьями 18.1. и 19 Федерального закона «О персональных данных»**	**Организационные меры:** - Назначен ответственный за организацию обработки персональных данных. - Разработана и опубликована политика в отношении обработки персональных данных. - Разработаны и введены в действие «Положение об обеспечении безопасности персональных данных, обрабатываемых в информационных системах персональных данных», «Положение об организации обработки персональных данных», «Положение об организации обработки персональных данных, без использования средств автоматизации». - Определены уровни защищенности персональных данных при их обработке в информационных системах персональных данных в зависимости от угроз безопасности этих данных. - Ведется учет машинных носителей персональных данных. - По фактам несанкционированного доступа к персональным данным проводятся разбирательства в соответствии с «Регламентом реагирования на инциденты информационной безопасности в информационных системах персональных данных». - Установлены правила доступа к персональным данным, обрабатываемым в информационных системах персональных данных, а также обеспечивается регистрация и учет всех действий пользователей, совершаемых с персональными данными в информационной системе персональных данных. - Проводится внутренний контроль соответствия обработки персональных данных требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных и локальным актам оператора. - Работники, непосредственно осуществляющие обработку персональных данных, ознакомлены с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных - Проводится обучение работников, использующих средства защиты информации, применяемые в информационных системах персональных данных, правилам работы с ними. **Средства обеспечения безопасности *(ниже указан пример заполнения):*** - Для хранения носителей информации с персональными данными используются запирающиеся шкафы и сейфы. - - Помещения, в которых проводится обработка персональных данных, оборудованы запирающимися дверьми, пожарной сигнализацией. Ведется видеонаблюдение по периметру здания, в коридорах. - Разграничение доступа пользователей к информационным системам персональных данных осуществляется с помощью доменных политик Active Directory *(если есть)*. - Применяются средства антивирусной защиты информации. - Применяется SSL-шифрование информации для обеспечения безопасности персональных данных при передаче по открытым каналам связи. - Применяются средства межсетевого экранирования.

8	**Сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством РФ**	- Утвержден руководителем оператора документ, определяющий перечень лиц, допущенных к обработке персональных данных, для выполнения ими служебных (трудовых) обязанностей. - Определены места хранения персональных данных (материальных носителей), обеспечивается раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях. При хранении материальных носителей соблюдаются условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ. - Организован режим обеспечения безопасности помещений, в которых размещены информационные системы персональных данных и проводится неавтоматизированная обработка персональных данных, препятствующий возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения. - Назначено должностное лицо (работник), ответственный за обеспечение безопасности персональных данных в информационных системах персональных данных. - Персональные данные обрабатывается в соответствии с требованиями внутренних нормативных документов, регламентирующих порядок хранения, обработки и защиты персональных данных. - Используются средства защиты информации, прошедшие процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз. - Контроль за выполнением требований по защите персональных данных организуется и проводится оператором не реже 1 раза в 3 года самостоятельно и с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации.
9	**Дата начала обработки персональных данных**	Дата начала обработки персональных данных в Вашей организации.
10	**Срок или условие прекращения обработки персональных данных**	Прекращение обучения ребенка; прекращение работы педагога в образовательном учреждении.
11	**Перечень действий с персональными данными, общее описание используемых оператором способов обработки персональных данных**	Сбор, запись, систематизация, уточнение (обновление, изменение), извлечение, использование, передача (распространение, предоставление, доступ), блокирование, удаление, уничтожение. Накопление и хранение осуществляется в серверном сегменте АИС «Региональный Навигатор…» *(указать официальное название АИС «Навигатор» в Вашем регионе)*
12	**Обработка вышеуказанных персональных данных будет осуществляться путем**	**Автоматизированная*, с передачей по внутренней сети юридического лица, с передачей по сети Интернет** **** - Если данные из АИС «Навигатор» дублируются на бумажных носителях, то вместо "автоматизированная" необходимо указывать "смешанная".***
	Категории персональных данных	

13	**Персональные данные**	ФИО ребенка, Дата рождения ребенка, СНИЛС ребенка, Номер сертификата персонифицированного финансирования дополнительного образования ребенка; ФИО родителя, Email родителя, Телефон родителя, Муниципалитет родителя, ФИО детей; ФИО педагога, Дата рождения педагога, Образование педагога, Наличие ученой степени педагога, Должность педагога, Email педагога, Телефон педагога, Даты приема на работу и увольнения педагога.
14	**Специальные категории персональных данных**	Нет
15	**Категории субъектов, персональные данные которых обрабатываются**	Дети, по которым подаются заявки на обучение; Родители подающие заявки на обучение по своим детям; Педагоги образовательных учреждений, участвующих в обучении детей.
16	**Осуществление трансграничной передачи персональных данных**	Не осуществляется
17	**Использование шифровальных (криптографических) средств**	Не используются
18	**Сведения о местонахождении базы данных информации, содержащей персональные данные граждан РФ**	Датацентр Colocat-Кунцево: 121351, г. Москва, ул. Молодогвардейская, 52 строение 2
19	**База данных № 1**	
	Страна	Россия
20	**Адрес ЦОДа**	Адрес Вашей организации
21	**Собственный ЦОД**	Да
	Нажмите «Добавить сведения»	
22	**База данных № 2**	
	Страна	Россия
23	**Адрес ЦОДа**	Датацентр Colocat-Кунцево: 121351, г. Москва, ул. Молодогвардейская, 52 строение 2
24	**Собственный ЦОД**	Нет
	Сведения об организации, ответственной за хранение данных	
25	**Тип организации**	Юридическое лицо
26	**Организационно-правовая форма**	Общество с ограниченной ответственностью
27	**Наименование организации**	«Государство Детей»
28	**ОГРН / ИНН**	1147746809704 / 7718989746
29	**Страна / Адрес местонахождения**	Россия / 129085, г. Москва, Звездный бульвар, д. 19, стр. 1, офис 1201
	Ответственный за организацию обработки персональных данных	
30	**Физическое лицо**	

31	**ФИО, почтовый адрес, номера контактных телефонов, адрес электронной почтой**	В соответствии с данными сотрудника – должно совпадать с данными, указанными в анкете для ОРД или самих организационно-распорядительных документах.
32	**ФИО исполнителя, должность, контактная информация**	В соответствии с данными сотрудника