УТВЕРЖДАЮ
Директор МБОУ «Свияжская СОШ ЗМР РТ»

Вавилова Н.А.

Введено в действие приказом
№ 224 от 10.08.2019г.

Регламент обеспечения информационной безопасности персональных данных МБОУ «Свияжская СОШ ЗМР РТ» при взаимодействии с контрагентами и третьими лицами при работе в государственной информационной системе Республики Татарстан «Бухгалтерский учет и отчетность государственных органов Республики Татарстан и подведомственных им учреждений»

ИСПОЛЬЗУЕМЫЕ СОКРАЩЕНИЯ

Сокращение	Полное наименование
Департамент	Департамент казначейства Министерства финансов Республики Татарстан
Система	Государственная информационная система Республики Татарстан «Бухгалтерский учет и отчетность государственных органов Республики Татарстан и подведомственных им учреждений»
ИБ	Информационная безопасность
МИС РТ	Министерство информатизации и связи Республики Татарстан
Орган	Органы государственной власти/ Органы местного самоуправления/Подведомственные учреждения
ПДн	Персональные данные
ппо	Прикладное программное обеспечение

1.ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий документ устанавливает порядок обеспечения ИБ ПДн в Системе и выполнения положений Закона при взаимодействии с контрагентами и третьими лицами.

1.2. Данный Регламент охватывает следующие случаи взаимодействия с контрагентами и третьими лицами в процессе обработки ПДн:

- обмен ПДн с контрагентами и третьими лицами;
- предоставление доступа к Системе контрагентам и третьим лицам.

1.3. Обмен ПДн между Департаментом, Органом и контрагентами и третьими лицами может происходить в случаях, установленных федеральным законодательством Российской Федерации с соблюдением установленных норм защиты ПДн.

2. ОБЯЗАННОСТИ И ОТВЕТСТВЕННОСТЬ РАБОТНИКОВ

2.1 В рамках обеспечения ИБ ПДн при взаимодействии с контрагентами и третьими лицами выделяются следующие роли:

-руководители структурных подразделений, в которых работают пользователи Системы;

-ответственный за обеспечение безопасности ПДн;

-администратор ППО (администратор пользователей учреждения);

-администратор безопасности (СИС админ);

-пользователи.

2.2 На ответственных за обеспечение безопасности ПДн в Департаменте, Органах, осуществляющих обработку ПДн, возлагаются следующие обязанности:

1) проведение инструктажа пользователей Системы (под роспись в «Журнале проведения инструктажа»), для ознакомления со следующими документами:

- правила обеспечения безопасности персональных данных при их обработке; - регламент обеспечения информационной безопасности персональных данных при взаимодействии с контрагентами и третьими лицами;

- регламент выгрузки и передачи персональных данных.

2) учет работников своего подразделения, допущенных к обработке ПДн Системы;

3) обеспечение выполнения пользователями Системы требований документов:

- правила обеспечения безопасности персональных данных при их обработке;

-регламент обеспечения информационной безопасности персональных данных при взаимодействии с контрагентами и третьими лицами;

-регламент выгрузки и передачи персональных данных.

2.3 На ответственного за обеспечение безопасности ПДн возлагаются следующие обязанности:

-планирование и координация работ по обеспечению безопасности ПДн Системы;

-контроль реализации организационных и технических мер обеспечения информационной безопасности ПДн Системы;

-контроль выполнения пользователями, обрабатывающими ПДн в рамках Системы, установленных правил по их защите ПДн при обработке;

-организация технической реализации требований по защите ПДн Системы.

2.4 В рамках деятельности по обеспечению безопасности ПДн на администраторов ППО возлагаются обязанности по обеспечению сопровождения и системного администрирования ППО, а также по предоставлению доступа пользователям к Системе.

2.5 В рамках деятельности, обязанность по контролю соблюдения мер по защите ПДн при их обработке возлагаются на ответственного за обеспечение безопасности ПДн Системы. .

2.6 На пользователей, обрабатывающих ПДн в рамках Системы, возлагаются обязанности по соблюдению положений организационно-распорядительной документации в части обеспечения защиты ПДн в рамках Системы в части их касающейся.

получения ПДн, указанный орган направляет письменный запрос на получение данных сведений руководству Департамента, Органу.

4.4 Запрос должен быть оформлен на официальных бланках с подписью руководителей запрашивающих органов и должен содержать указание цели и правовое основание требования ПДн, если иное не установлено Федеральными Законами. Запрос также может содержать описание порядка (формы, сроки и способы) передачи ПДн.

4.5 При принятии решения об удовлетворении запроса руководителем Департамента, руководителем Органа, осуществляется предоставление ПДн в соответствии с разделами 7, 8 настоящего Регламента.

4.6. Руководитель структурного подразделения, в котором работают пользователи Системы, уведомляет Ответственного за обеспечение безопасности ПДн в Системе о факте передачи ПДн.

5. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ОБМЕНЕ ПЕРСОНАЛЬНЫМИ ДАННЫМИ В РАМКАХ ЗАКЛЮЧЕННЫХ ДОГОВОРОВ

5.1 При возникновении необходимости заключения договора об обмене ПДн с контрагентами в Системе обязательным является согласование вопроса с Департаментом и с МИС РТ.

5.2 Обмен ПДн с контрагентами в рамках заключенных договоров через структурные подразделения Органов запрещен.

5.3 В случае если обмен ПДн субъектов ПДн с контрагентами осуществляется на основании договора между Департаментом и контрагентом, условия предоставления ПДн определяются в данном договоре.

5.4 При заключении договора с контрагентом в договор вносятся условия предоставления ПДн и обязательства контрагента по обеспечению безопасности ПДн (в том числе в случае реорганизации или ликвидации организации-контрагента), а также заключается Соглашение о конфиденциальности с контрагентами, которым передаются ПДн.

5.5 Условия предоставления ПДн и обязательства контрагента по обеспечению безопасности ПДн, включаемые в состав договора, согласовываются с Ответственным за обеспечение безопасности ПДн в Системе.

5.6. Передача (получение) ПДн осуществляется в соответствии с разделами 7, 8 настоящего Регламента.

6. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ПЕРЕДАЧЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1 Передача ПДн осуществляется на материальном носителе или в электронном виде по каналам связи, ответственным за работу с ПДн в Департаменте, Органе по решению руководителя Департамента, Органа.

6.2 Передача ПДн на материальном носителе осуществляется в следующем порядке:

6.2.1 Департамент, Орган, в котором работают пользователи Системы, проставляют на передаваемых документах, содержащих ПДн, отметку «конфиденциально», либо «Для служебного пользования». Передача документов осуществляется сопроводительным письмом с уведомлением контрагента или третьего лица о конфиденциальности передаваемых данных, а также с запросом на подтверждение получения передаваемых данных. Рекомендуемая форма сопроводительного письма приведена в приложении №1.

6.2.2 Сопроводительное письмо подписывается руководителем Департамента, органа либо его заместителем, и прикладывается к передаваемому материальному носителю.

- меры по снижению категории или объема ПДн путем редактирования, обезличивания или сегментирования полученных файловых массивов.

7.6 Применяемые меры и средства защиты информации должны обеспечивать соответствие Системы требованиям норм и стандартов в области обеспечения ИБ. Соответствие нормам и стандартам ИБ должно быть подтверждено оценкой соответствия в форме аттестации на соответствие требованиям ИБ.

7.7 Ответственный за обеспечение безопасности ПДн от учреждения определяет ответственных за реализацию данных мер, в том числе в рамках действующих договоров с сервисными организациями.

7.8. Загрузку ПДн в Систему осуществляют администраторы Системы в соответствии с эксплуатационной документацией на систему.

8. ПРЕДОСТАВЛЕНИЕ КОНТРАГЕНТАМ ДОСТУПА К ИНФОРМАЦИОННОЙ СИСТЕМЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

8.1 Предоставление доступа к Системе осуществляется на основании договора, заключенного между Департаментом, МИС РТ и контрагентом, в котором определяются условия предоставления доступа к ПДн.

8.2 При заключении договора с контрагентом в договор вносятся условия предоставления доступа к Системе и обязательства контрагента по обеспечению безопасности ПДн (в том числе в случае реорганизации или ликвидации организации-контрагента), а также заключается Соглашение о конфиденциальности с контрагентами, которые могут получить доступ к ПДн.

8.3 Предоставление представителям контрагентов доступа к Системе осуществляется на основании письма контрагента, которому необходимо предоставить доступ. В письме указываются координаты ответственного лица контрагента.

8.4 На основании заключенного договора, указанного в п.8.1. настоящего раздела, Ответственный за обеспечение безопасности ПДн вносит данные о контрагенте в Список контрагентов и третьих лиц, имеющих доступ к Системе (далее - Список) (Форма Списка представлена в Приложении №2).

8.4.1 Список контрагентов и третьих лиц, имеющих доступ к Системе, хранится у Ответственного за обеспечение безопасности ПДн от учреждения, или назначенного им ответственного лица.

8.4.2 Данный список передается системному администратору, отвечающему за техническую эксплуатацию Системы.

8.4.3 Предоставление доступа к Системе контрагентам и третьим лицам осуществляется в следующем порядке:

Администратор ППО проверяет, существует ли техническая возможность предоставления доступа.

В случае если такая возможность существует, администратор ППО формирует технические условия и требования, при которых возможно предоставление прав доступа. Данные условия и требования должны распространяться как на Стороны заключенного договора.

8.4.4 Требования и технические условия определяются для каждого конкретного случая, но в общем случае должны включать:

- необходимые технические условия (требования к параметрам соединений, необходимая конфигурация и настройки оборудования, требования к средствам защиты информации, требование отсутствия подключения к другим сетям или меры по защите, применяемые при подключении и т.д.);
- требования по защите информации, которые должны соблюдаться организацией-контрагентом;

Приложение 1

Рекомендуемая форма сопроводительного письма

В ответ на Ваш запрос от «_____» _____20 __ г. (на основании Договора № _____) в Ваш адрес направляю персональные данные о _____
(прилагаются).

В соответствии с Федеральным Законом № 152 «О персональных данных» передаваемая Вам информация является конфиденциальной.

В соответствии с действующим законодательством Российской Федерации на Вас возлагаются обязательства по обеспечению безопасности персональных данных (в том числе по недопущению их незаконного распространения) с даты предоставления их Вам.

Просим подтвердить получение Вами переданных сведений в письменной форме.

_____	_____	_____
(наименование должности должностного лица Органа)	(подпись)	(ФИО)

Приложение 3

ЖУРНАЛ УЧЕТА НАРУШЕНИЙ ПОРЯДКА ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ ГОСУДАРСТВЕННОЙ ИНФОРМАИОННОЙ СИСТЕМЫ «БУХГАЛТЕРСКИЙ УЧЕТ И ОТЧЕТНОСТЬ ГОСУДАРСТВЕННЫХ ОРГАНОВ РЕСПУБЛИКИ ТАТАРТАН И ПОДВЕДОМСТВЕННЫХ ИМ УЧРЕЖДЕНИЙ»

Начат «___»_____20__г.
Окончен «___»_____20__г.

№	Дата выявления нарушения	ФИО и подпись работника, выявившего нарушение	Описание нарушения	Предпринятые действия	Примечание