УТВЕРЖДЕНО
Постановлением Администрации
Прионежского муниципального района
от «____»_____ 2021 года № _____

ПРАВИЛА

осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в Администрации Прионежского муниципального района

1. Общие положения

1.1. Настоящие правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее - Правила) в Администрации Прионежского муниципального района (далее - Администрация), определяют порядок выявления и предотвращения нарушений, законодательства Российской Федерации в сфере обработки персональных данных (далее — ПДн), а также основания, формы и методы проведения внутреннего контроля соответствия обработки ПДн требованиям к защите персональных данных.

1.2. Настоящие Правила разработаны на основании Федерального закона Российской Федерации от 27.07. 2006 г. № 152-ФЗ «О персональных данных» и в соответствии с Перечнем мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами, утвержденными постановлением Правительства Российской Федерации от 21.03. 2012 г. № 211.

1.3. Для обработки ПДн, необходимых для предоставления государственных и муниципальных услуг, а также для обработки ПДн сотрудников используются в Администрации информационные системы персональных данных (далее - ИСПДн).

1.4. Пользователем ИСПДн (далее - Пользователь) является работник Администрации, участвующий в рамках выполнения своих функциональных обязанностей в процессах автоматизированной обработки ПДн и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты информации ИСПДн.

1.5. Контрольные мероприятия для обеспечения уровня защищенности персональных данных и соблюдения условий использования средств защиты информации, а также соблюдения требований законодательства Российской

Федерации по обработке персональных данных в ИСПДн Администрации проводятся в следующих целях:

— проверка выполнения требований организационно-распорядительной документации по защите информации в Администрации, действующего законодательства Российской Федерации в области обработки и защиты персональных данных;

— оценка уровня осведомленности и знаний работников Администрации в области обработки и защиты персональных данных; оценка обоснованности и эффективности применяемых мер и средств защиты.

2. Тематика внутреннего контроля

Тематика внутреннего контроля соответствия обработки ПДн требованиям к защите ПДн:

2.1. Проверки соответствия обработки ПДн установленным требованиям в Администрации разделяются на следующие виды:

- регулярные;
- плановые;
- внеплановые.

2.2. Регулярные контрольные мероприятия проводятся Администратором безопасности в соответствии с утвержденным Планом внутренних проверок контроля соответствия обработки персональных данных требованиям к защите персональных данных и предназначены для осуществления контроля выполнения требований в области защиты информации в Администрации.

2.3. Плановые контрольные мероприятия проводятся комиссией в соответствии с утвержденным Планом и направлены на постоянное совершенствование системы защиты персональных данных ИСПДн в Администрации.

2.4. Внеплановые контрольные мероприятия могут проводится на основании решения комиссии по информационной безопасности, создаваемой на период проведения мероприятий. Решение о проведении внеплановых контрольных мероприятий и создании комиссии может быть принято в следующих случаях:

— по результатам расследования инцидента информационной безопасности;

— по результатам внешних контрольных мероприятий, проводимых регулирующими органами;

— по решению Главы Администрации.

3. Планирование контрольных мероприятий

3.1. Для проведения плановых внутренних контрольных мероприятий Администратор безопасности, разрабатывает План внутренних контрольных мероприятий на текущий год.

3.2. План проведения внутренних контрольных мероприятий включает следующие сведения по каждому из мероприятий:

— цели проведения контрольных мероприятий;

— задачи проведения контрольных мероприятий;

— объекты контроля (процессы, подразделения, информационные системы персональных данных и т.п.);

— состав участников, привлекаемых для проведения контрольных мероприятий;

— сроки и этапы проведения контрольных мероприятий;

3.3. Общий срок контрольных мероприятий не должен превышать пяти рабочих дней. При необходимости срок проведения контрольных мероприятий может быть продлен, но не более чем на десять рабочих дней, соответствующие изменения отображаются в Отчете, выполняемом по результатам проведенных контрольных мероприятий.

4. Оформление результатов контрольных мероприятий

4.1. По итогам проведения регулярных контрольных мероприятий результаты проверок фиксируются в Журнале учета событий информационной безопасности.

4.2. По итогам проведения плановых и внеплановых контрольных мероприятий, комиссия разрабатывает отчет, в котором указывается:

1) описание проведенных мероприятий по каждому из этапов;

2) перечень и описание выявленных нарушений;

3) рекомендации по устранению выявленных нарушений;

4) заключение по итогам проведения внутреннего контрольного мероприятия.

4.3. Отчет передается на рассмотрение Главе Администрации.

4.4. Общая информация о проведенном контрольном мероприятий фиксируется в Журнале учета событий информационной безопасности.

4.5. Результаты проведения мероприятий по внеплановому контролю заносятся в протокол проведения внутренних проверок контроля соответствия обработки персональных данных требованиям к защите персональных данных в Администрации.

5. Порядок проведения плановых и внеплановых контрольных мероприятий

5.1. Плановые и внеплановые контрольные мероприятия проводятся при обязательном участии Администратора безопасности, к проведению контрольных мероприятий может привлекаться ответственный за организацию обработки ПДн в Администрации.

5.2. Лицо, ответственное за обеспечение безопасности ПДн (Администратор безопасности), не позднее чем за три рабочих дня до начала проведения контрольных мероприятий уведомляет всех руководителей подразделений, в которых планируется проведение контрольных мероприятий, и направляет им для ознакомления План проведения контрольных мероприятий. При проведении внеплановых контрольных мероприятий уведомление не требуется.

5.3. Во время проведения контрольных мероприятий, в зависимости от целей мероприятий, могут выполнятся следующие проверки:

- соответствие полномочий пользователя правилам доступа к персональным данным.
- соблюдение пользователями требований инструкций по организации антивирусной и парольной защиты, инструкции по обеспечению безопасности персональных данных.
- соблюдение Администратором безопасности и инженером-электроником инструкций и регламентов по обеспечению безопасности информации в Администрации.
- соблюдение Порядка доступа в помещения Администрации, где ведется обработка персональных данных.
- знание пользователем Инструкции по работе в ИСПДн.
- знание Администратором безопасности инструкций и регламентов по обеспечению безопасности информации в Администрации.
- порядок и условия применения средств защиты информации.
- состояние учета машинных носителей персональных данных.
- наличие фактов несанкционированного доступа к ПДн и принятие необходимых мер.
- проведенные мероприятия по восстановлению ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.
- технические мероприятия, связанные с штатным и нештатным функционированием средств защиты.