

Приложение № 5  
к приказу ГКУ АО «Центр социальной  
поддержки населения Приволжского  
района» от 20.12.2019 № 284/01-12

**ПРАВИЛА ОСУЩЕСТВЛЕНИЯ ВНУТРЕННЕГО КОНТРОЛЯ  
СООТВЕТСТВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ  
ТРЕБОВАНИЯМ К ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В  
ГКУ АО «ЦЕНТР СОЦИАЛЬНОЙ ПОДДЕРЖКИ НАСЕЛЕНИЯ  
ПРИВОЛЖСКОГО РАЙОНА»**

Настоящими Правилами осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее - Правила) в ГКУ АО «Центр социальной поддержки населения Приволжского района» (далее - Учреждение) определяются процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных; основания, порядок и сроки проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.

В настоящих Правилах используются основные понятия, определенные в статье 3 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

Осуществление внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в Учреждении выполняется специалистами информационно-аналитического сектора и отдела организационно-правовой работы и развития трудовых отношений, путём контроля состояния технической защиты информации (порядка функционирования средств технической защиты информации, соблюдения установленных режимов работы объектов информатизации, выполнения установленных мер технической защиты информации, в том числе от НСД) и выполнения требований законодательных, нормативно-правовых, организационно - распорядительных и методических документов как федерального уровня, так и принятых в Учреждении, в области защиты информации.

В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям в Учреждении организуется проведение периодических проверок условий обработки персональных данных.

Проверки осуществляются ответственными лицами за организацию обработки персональных данных в Учреждении, администратором безопасности информации либо комиссией, созданной на основании приказа директора Учреждения.

В проведении проверки не может участвовать сотрудник Учреждения, прямо или косвенно заинтересованный в ее результатах.

Проверки соответствия обработки персональных данных установленным требованиям в Учреждении могут быть как плановыми, так и внеплановыми.

Плановые проверки проводятся на основании утвержденного Плана внутренних проверок условий обработки персональных данных в учреждении, результаты проверок заносятся в Журнал учета внутренних проверок условий обработки персональных данных в учреждении.

Проведение внеплановой проверки организуется в течение трех рабочих дней с момента поступления соответствующего заявления. Внеплановая проверка должна быть завершена не позднее чем через месяц со дня принятия решения о ее проведении. По результатам проведенной проверки составляется Акт, в котором указывается перечень мер, необходимых для устранения выявленных нарушений.

При проведении проверки соответствия обработки персональных данных установленным требованиям должны быть полностью, объективно и всесторонне установлены:

- порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;

- порядок и условия применения средств защиты информации;

- эффективность принимаемых мер по обеспечению безопасности персональных данных, обрабатываемых в информационной системе персональных данных;

- состояние учета машинных носителей персональных данных;

- соблюдение правил доступа к персональным данным;

- наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер;

- осуществление мероприятий по обеспечению целостности персональных данных.

Ответственный за организацию обработки персональных данных в Учреждении (члены комиссии) имеет право:

- запрашивать у сотрудников Учреждения информацию, необходимую для реализации полномочий;

- требовать от уполномоченных на обработку персональных данных должностных лиц уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;

- принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства Российской Федерации;

- представлять директору Учреждения предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке;

- представлять директору Учреждения предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в отношении обработки персональных данных.

В процессе проведения проверки необходимо установить обстоятельства нарушения, в т.ч. времени, места и способа его совершения, установить лиц виновных в данном нарушении, провести разработку и принятие мер по предотвращению возможных негативных последствий подобных нарушений.

В отношении персональных данных, ставших известными ответственному за организацию обработки персональных данных, администратору безопасности информации либо членам комиссии в Учреждении в ходе проведения мероприятий внутреннего контроля, должна обеспечиваться конфиденциальность персональных данных.