УТВЕРЖДАЮ
Директор ГБУ СО ЯО
Краснoперекопский
психоневрологический
интернат

_____М.В.Филиппова
«10» 04 2020 г.

ПРАВИЛА
осуществления внутреннего контроля соответствия обработки персональных данных в государственном учреждении социального обслуживания Ярославской области Краснoперекопский психоневрологический интернат

1. Общие положения

1. Правила осуществления внутреннего контроля соответствия обработки персональных данных в государственном учреждении социального обслуживания Ярославской области Краснoперекопский психоневрологический интернат (далее – Правила) определяют порядок организации и осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в государственном учреждении социального обслуживания Ярославской области Краснoперекопский психоневрологический интернат (далее – Учреждение).

2. Настоящие Правила разработаны в соответствии с Федеральным законом от 27.07.2006№152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ), Федеральным законом от 02.05.2006 г. № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации», постановлением Правительства Российской Федерации от 21.03.2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами в сфере защиты персональных данных.

3. Внутренний контроль соответствия обработки персональных данных требованиям к защите персональных данных (далее – внутренний контроль) в

Учреждении осуществляется с целью определения наличия несоответствий между требуемым уровнем защиты персональных данных и его фактическим состоянием, а также выработки мер по их устранению и недопущению в дальнейшем.

2. Порядок проведения проверки

2.1. Внутренний контроль осуществляется комиссией по проведению внутреннего контроля соответствия обработки персональных данных в Учреждении требованиям к защите персональных данных (далее – комиссия) путѐм проведения проверок. Состав комиссии утверждается приказом директора Учреждения.

2.2. Внутренний контроль проводится в форме плановых и внеплановых проверок.

2.3.Плановые проверки соответствия обработки персональных данных установленным требованиям проводятся не чаще чем один раз в 6 месяцев (2 раза в год) в соответствии с утвержденным планом. План проведения внутреннего контроля на очередной год утверждается директором Учреждения.

2.4.Внеплановые проверки могут быть контрольными и по частным вопросам:

2.4.1. Контрольные проверки проводятся для установления полноты выполнения рекомендаций плановых проверок.

2.4.2. Проверки по частным вопросам охватывают отдельные направления по защите персональных данных и могут проводиться в случаях, когда стали известны факты несанкционированного доступа, утечки либо утраты персональных данных субъектов персональных данных Учреждения или нарушения требований по защите персональных данных.

2.5. В ходе осуществления контроля выполнения требований по защите персональных данных в Учреждении проверке могут подлежать следующие показатели:

2.5.1. В части общей организации работ по защите персональных данных:

- соответствие информации, указанной в уведомлении об обработке персональных данных, реальному положению дел;
- наличие нормативных документов по защите персональных данных;
- знание нормативных документов сотрудниками, имеющими доступ к персональным данным;
- полнота и правильность выполнения требований нормативных документов сотрудниками, имеющими доступ к персональным данным;

- наличие лиц, назначенных ответственными за организацию обработки персональных данных в структурном подразделении, уровень их профессиональной подготовки и способность выполнить возложенные обязанности;

- наличие согласий на обработку персональных данных субъектов персональных данных. Соответствие объёма персональных данных и сроков обработки целям обработки персональных данных;

- соответствие схемы контролируемой зоны, перечня мест хранения материальных носителей, перечня лиц, допущенных к обработке персональных данных, фактическому состоянию.

2.5.2. В части защиты персональных данных в информационных системах персональных данных (далее – ИСПДн):

- соответствие средств вычислительной техники ИСПДн показателям, указанным в документации на ИСПДн;

- структура и состав локальных вычислительных сетей, организация разграничения доступа пользователей к сетевым информационным ресурсам, порядок защиты охраняемых сведений при передаче (обмене) персональных данных в сети передачи данных (СПД);

- контроль целостности пломб на аппаратных средствах, с которыми осуществляется штатное функционирование средств криптографической защиты информации;

- соблюдение установленного порядка использования средств вычислительной техники ИСПДн;

- наличие и эффективность применения средств и методов защиты персональных данных, обрабатываемых на средствах электронно-вычислительной техники (ЭВТ);

- соблюдение требований, предъявляемых к паролям на информационные ресурсы;

- соблюдение требований и правил антивирусной защиты персональной электронно-вычислительной машины (ПЭВМ) и программ;

- контроль журналов учёта носителей персональных данных. Сверка основного журнала с дублирующим (если требуется ведение дублирующего учёта носителей).

2.5.3. В части защиты информационных ресурсов и помещений:

- правильность отнесения обрабатываемой информации к персональным данным;

- правильность классификации информационной системы;

- закрепление гражданско-правовой ответственности в сфере информационной безопасности и соблюдения режима конфиденциальности персональных данных в правилах внутреннего трудового распорядка,

положениях учреждения, должностных инструкциях сотрудников и трудовых договорах;

- порядок передачи персональных данных органам государственной власти, местного самоуправления и сторонним организациям (контрагентам);

- состояние конфиденциального делопроизводства, соблюдение установленного порядка подготовки, учѐта, использования, хранения и уничтожения документов, содержащих персональные данные;

- выполнение требований по правильному оборудованию защищаемых помещений и предотвращению утечки охраняемых сведений при проведении мероприятий конфиденциального характера;

- соответствие защищаемых помещений их техническим паспортам.

2.6. Ответственные за организацию обработки персональных данных в ходе проверки имеют право:

– запрашивать у работников информацию, необходимую для реализации своих 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;

– вносить предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке;

– вносить предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в отношении обработки персональных данных.

2.7.В ходе работы проверяющие лица должны принимать меры по устранению на месте отмечаемых нарушений и недостатков. Недостатки, которые не могут быть устранены на месте, включаются в итоговый документ по результатам проверки.

3. Оформление результатов проверки

3.1.Результаты проверки оформляются в виде акта внутреннего контроля, который подписывается членами комиссии в количестве не менее 3-х человек.

3.2.Результаты проверок подразделений периодически обобщаются в виде отчета.