УТВЕРЖДЕНЫ
приказом директора
ОГБУ «КЦСО ЕАО»

от «09» февраля 2021 г. № 54

ПРАВИЛА
осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных
в ОГБУ «Комплексный центр социального обслуживания Еврейской автономной области»

1. Общие положения

1.1. Настоящие Правила осуществления внутреннего контроля соответствия обработки и защиты персональных данных требованиям к защите персональных данных в ОГБУ «Комплексный центр социального обслуживания Еврейской автономной области» (далее – Учреждение) определяют основания, порядок и формы проведения внутреннего контроля.

1.2. Настоящие Правила разработаны в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами и внутренними локальными актами Учреждения.

1.3. Целями осуществления внутреннего контроля являются:

- оценка общего состояния выполнения требований по обработке и защите персональных данных в Учреждении;
- выявление и предотвращение нарушений законодательства в сфере персональных данных.

2. Порядок осуществления внутреннего контроля

2.1. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям Учреждение организует проведение периодических проверок условий обработки персональных данных.

2.2. Проверки осуществляются комиссией по проведению внутренних проверок либо ответственным за организацию обработки персональных данных (далее – Ответственный) как непосредственно на месте обработки

персональных данных путём опроса и осмотра рабочих мест должностных лиц, участвующих в процессе обработки персональных данных, так и путём направления запросов и рассмотрения документов, необходимых для осуществления внутреннего контроля.

2.3. Проверки соответствия обработки и защиты персональных данных установленным требованиям разделяются на:

- плановые;
- внеплановые.

2.4. Плановые проверки соответствия обработки персональных данных установленным требованиям проводятся не реже одного раза в год в каждом структурном подразделении Учреждения.

2.5. Плановые проверки проводятся в соответствии с Планом внутренних проверок, который формируется на очередной год Ответственным либо Председателем комиссии и утверждается директором Учреждения. При необходимости План может корректироваться.

2.6. План внутренних проверок составляется в декабре текущего года на следующий год.

2.7. По результатам каждой проверки составляется Акт проведения внутренней проверки, который подписывается членами комиссии в количестве не менее 3-х человек и утверждается председателем комиссии.

2.8. При выявлении нарушений в ходе проверки Ответственным либо Председателем комиссии в Акте делается запись о мероприятиях по устранению нарушений и сроках исполнения.

2.9. Акты хранятся у Ответственного либо Председателя комиссии в течение текущего года. Уничтожение Актов проводится Ответственным самостоятельно в январе следующего за отчётным года.

2.10. Внеплановые проверки проводятся на основании решения комиссии по проведению внутренних проверок в следующих случаях:

- по результатам расследования выявленных нарушений требований законодательства в сфере защиты персональных данных;
- по результатам внешних контрольных мероприятий, проводимых регулирующими органами;
- по решению руководителя Учреждения.

2.11. О результатах внутренней проверки и мерах, необходимых для устранения нарушений, руководителю докладывает Ответственный либо Председатель комиссии.

2.12. Общий срок внутренней проверки не должен превышать 10 (десяти) рабочих дней. При необходимости срок проведения проверки может быть продлён, но не более чем на 10 (десять) рабочих дней.

3. Перечень параметров проверок в области обеспечения безопасности персональных данных

3.1. При осуществлении внутреннего контроля соответствия обработки персональных данных установленным требованиям, производится:

– проверка актуальности сведений, содержащихся в уведомлении Учреждения об обработке персональных данных (сайт Роскомнадзора);

– проверка актуальности локальных актов Учреждения в области обеспечения безопасности персональных данных;

– проверка актуальности перечня должностей работников Учреждения, замещение которых предусматривает осуществление обработки персональных данных, либо осуществление доступа к персональным данным;

– проверка знания и соблюдения работниками положений действующего законодательства Российской Федерации и локальных актов Учреждения в области обработки и обеспечения безопасности персональных данных;

– проверка правильности осуществления сбора, систематизации, записи, накопления, хранения, уточнения (обновления, изменения), извлечения, использования, передачи (распространения, предоставления, доступа), обезличивания, блокирования, удаления, уничтожения персональных данных в ИСПДн Учреждения;

– проверка наличия Согласий субъектов персональных данных, чьи персональные данные обрабатываются в информационных системах персональных данных Учреждения;

– проверка соблюдения порядка правил хранения и работы с бумажными носителями персональных данных;

– проверка соблюдения сроков хранения и порядка уничтожения персональных данных;

– проверка актуальности перечня ИСПДн в Учреждении;

– проверка выполнения работниками Учреждения требований и правил обработки персональных данных в информационных системах персональных данных;

– выборочные проверки работников на предмет знания организационно-распорядительных документов в области обработки и обеспечения безопасности персональных данных;

– подтверждение факта ознакомления работника с локальными актами Учреждения в области обработки и обеспечения безопасности персональных данных (листы ознакомления);

– проверка соблюдения пользователями информационных систем персональных данных парольной политики;

– проверка соблюдения пользователями информационных систем персональных данных антивирусной политики;

– проверка соблюдения пользователями информационных систем персональных данных правил работы со съёмными носителями персональных данных;

– проверка соблюдения порядка доступа в помещения, где расположены элементы информационных систем персональных данных;

– проверка соблюдения порядка резервирования баз данных и хранения резервных копий;

– проверка соблюдения порядка работы со средствами защиты информации;

- иные вопросы.

3.2. В отношении персональных данных, ставших известными в ходе проведения мероприятий внутреннего контроля, должна обеспечиваться конфиденциальность.

4. Права Комиссии при проведении проверки.

4.1. Комиссия для реализации своих полномочий имеет право:

- запрашивать у работников Учреждения, ответственных за обработку персональных данных, необходимую информацию;

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

- принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемых с нарушением требований действующего законодательства, а также устранению выявленных нарушений выполнения требований к защите персональных данных в Учреждении;

- 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.

4.2. Проверки могут проводиться с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации.