Приложение 3

УТВЕРЖДЕНЫ
приказом ОГБУ
«Многопрофильный центр
реабилитации»
от 15.01.2024г. № 12

ПРАВИЛА
осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленные Федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и локальными актами в областном государственном бюджетном учреждении «Многопрофильный центр реабилитации»

1. Общие положения

Настоящие правила разработаны в соответствии с положениями Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, и определяют порядок организации и осуществления контроля выполнения соответствия обработки персональных данных (далее – ПДн) требованиям к защите ПДн в структурных подразделениях (отделах) областного государственного бюджетного учреждения «Многопрофильный центр реабилитации» (далее – Учреждение).

Правила обязательны для исполнения всеми должностными лицами Учреждения, осуществляющими контроль состояния защиты ПДн.

Контроль выполнения соответствия обработки ПДн требованиям к защите ПДн в структурных подразделениях (отделах) Учреждения осуществляется с целью определения наличия несоответствий между требуемым уровнем защиты ПДн и его фактическим состоянием, правильности обработки ПДн ответственными лицами в структурных подразделениях (отделах), а также выработать меры по их устранению и недопущению в дальнейшем.

Контроль осуществляет ответственный за организацию обработки ПДн (далее – Ответственный) в Учреждении.

Контроль проводится в форме плановых и внеплановых проверок. Внеплановые проверки могут быть контрольными и по частным вопросам.

Контрольные проверки проводятся для установления полноты выполнения рекомендаций плановых проверок.

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

Проверки осуществляются Ответственным Учреждения либо комиссией, образуемой директором.

Сроки проведения контрольных проверок доводятся руководителям проверяемых структурных подразделений (отделов) не позднее, чем за 24 часа до начала проверки.

Проверки по частным вопросам могут проводиться без уведомления руководителей проверяемых структурных подразделений (отделов).

Периодичность и сроки проведения плановых проверок структурных подразделений (отделов) Учреждения устанавливаются планом, утверждаемый директором. Рекомендованная форма плана внутренних проверок состояния защиты ПДн приведена в приложении к данному документу. Сроки проведения плановых проверок доводятся руководителям проверяемых структурных подразделений (отделов) не позднее, чем за 10 суток до начала проверки.

2. Порядок подготовки к проверке

Проверка проводится на основании приказа и утверждённого плана проверок директором. Ответственный Учреждения подготавливает предложения по составу комиссии, при необходимости. Проект приказа о проверке подготавливает Ответственный Учреждения.

Проверяющие лица (комиссия, при её наличии) и Ответственный Учреждения обязаны получить у руководителей проверяемых структурных подразделений (отделов) информацию об условиях обработки ПДн, необходимую для достижения целей проверки. Перед началом проверки они должны изучить материалы предыдущих проверок данного структурного подразделения (отдела).

3. Порядок проведения проверки

По прибытию в структурное подразделение (отдел) для проведения проверки председатель комиссии (при наличии) или Ответственный Учреждения прибывает к руководителю проверяемого структурного

подразделения (отдела) Учреждения, представляется ему и представляет других прибывших на проверку лиц (при наличии).

Руководитель проверяемого структурного подразделения (отдела) обязан оказывать содействие Ответственному Учреждения и комиссии по проверке (при наличии) и в случае необходимости, определяет должностное лицо, ответственное за сопровождение проверки.

На период проведения контрольных мероприятий обработку ПДн необходимо по возможности прекращать. Допуск проверяющих лиц к конкретным информационным ресурсам, защищаемым сведениям и техническим средствам должен исключать ознакомление проверяющих лиц с конкретными ПДн.

Общий порядок проведения проверки включает следующее:

1) получение документов о распределении обязанностей по обработке и защите ПДн, выявление ответственных за обработку и защиту ПДн и установление факта ознакомления работниками проверяемого структурного подразделения (отдела) со своей ответственностью;

2) получение при содействии работников проверяемого структурного подразделения (отдела) документов, касающихся обработки и защиты ПДн в данном структурном подразделении (отделе);

3) анализ полученной документации;

4) непосредственная проверка выполнения установленного порядка обработки и защиты ПДн и требований законодательства Российской Федерации в области защиты ПДн.

При этом согласовываются конкретные вопросы по объёму, содержанию, срокам проведения проверки, а также каких должностных лиц структурного подразделения (отдела) необходимо привлечь к проверке и какие объекты следует посетить.

В ходе осуществления контроля выполнения требований по обработке и защите ПДн в проверяемом структурном подразделении (отделе) Учреждения рассматриваются, в частности, следующие показатели:

1) в части общей организации работ по обработке ПДн:

а) соответствие информации, указанной в уведомлении об обработке ПДн Учреждения, реальному положению дел;

б) соответствие обрабатываемой и собираемой информации (ПДн), их полнота, в соответствии с нормативными правовыми актами и локальными актами, принятыми в Учреждении;

в) наличие нормативных документов по защите ПДн;

г) знание нормативных документов работниками, имеющими доступ к ПДн;

д) полнота и правильность выполнения требований нормативных документов работниками Учреждения, имеющими доступ к ПДн;

е) наличие документов, определяющих состав работников, ответственных за обработку ПДн в структурном подразделении (отделе), соответствие этих документов реальному штатному составу структурного подразделения (отдела), а также подтверждение факта ознакомления ответственных работников с данными документами;

ж) уровень подготовки работников, ответственных за обработку ПДн в структурном подразделении (отделе);

з) наличие необходимых, в соответствии с требованиями Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных» согласий на обработку ПДн субъектов ПДн. Соответствие объёма обрабатываемых ПДн и сроков их обработки к указанным целям обработки ПДн.

2) в части защиты информационных систем с защищаемой информацией:

а) соответствие средств вычислительной техники, средств защиты информации и программного обеспечения в информационных системах показателям, указанным в документации на конкретную информационную систему (технический паспорт);

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

в) соблюдение установленного порядка использования средств вычислительной техники информационной системы;

г) наличие и эффективность применения средств и методов защиты информации, обрабатываемых на средствах вычислительной техники информационной системы;

д) соблюдение требований, предъявляемых к паролям на информационные ресурсы, средствам вычислительной техники, в том числе и BIOS;

е) соблюдение требований и правил антивирусной защиты средств вычислительной техники;

ж) контроль журналов учёта машинных носителей защищаемой информации. Сверка основного журнала с дублирующим (если требуется ведение дублирующего учёта носителей);

з) тестирование реализации правил фильтрации межсетевого экрана, процесса регистрации, процесса идентификации и аутентификации запросов, процесса идентификации и аутентификации администратора межсетевого экрана, процесса регистрации действий администратора межсетевого экрана, процесса контроля за целостностью программной и информационной части, процедуры восстановления настроек межсетевого экрана.

3) в части защиты информационных ресурсов и помещений:

а) правильность отнесения обрабатываемой информации к защищаемой информации;

б) правильность установления уровня защищённости ПДн в информационных системах ПДн и (или) правильности установления класса защищённости в государственных (муниципальных) информационных системах, при обработке в них ПДн;

в) закрепление гражданско-правовой ответственности в сфере информационной безопасности и соблюдения режима конфиденциальности в правилах внутреннего трудового распорядка, положениях о структурных подразделениях (отделов) Учреждения, должностных инструкциях и трудовых договорах работников;

г) порядок передачи защищаемой информации органам государственной власти, местного самоуправления и сторонним организациям (контрагентам);

д) действенность принимаемых мер по защите охраняемых сведений в ходе подготовки материалов к открытому опубликованию и при изготовлении рекламной продукции;

е) состояние конфиденциального делопроизводства, соблюдение установленного порядка подготовки, учёта, использования, хранения и уничтожения документов, содержащих ПДн;

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

з) соответствие защищаемых помещений их техническим паспортам.

Более подробно вопросы, подлежащие проверке, могут раскрываться в отдельных документах (методических рекомендациях, технологических картах, памятках и т.п.).

Во время проведения проверки, выявленные нарушения требований по обработке и защите ПДн должны быть по возможности устранены. Проверяющие лица могут давать рекомендации по устранению на месте отмечаемых нарушений и недостатков.

Недостатки, которые не могут быть устранены на месте, включаются в итоговый документ по результатам проверки.

4. Оформление результатов проверки

Результаты проверки оформляются:

1) актом – при проведении проверки комиссией (при наличии);

2) служебной запиской – при проведении проверки Ответственным Учреждения.

Акт и (или) служебная записка составляется в двух экземплярах и подписывается работниками, выполнявших проверку.

Один экземпляр хранится у Ответственного Учреждения, второй экземпляр хранится в Учреждении в установленном порядке. Копия документа о проверке остается у руководителя (начальника) проверяемого структурного подразделения (отдела).

Результаты проверок структурных подразделений (отделов) периодически обобщаются Ответственным Учреждения и доводятся до руководителей структурных подразделений (отделов). При необходимости принятия решений по результатам проверок структурных подразделений (отделов) на имя директора готовятся соответствующие служебные записки.