ДЕПАРТАМЕНТ ОХРАНЫ ЗДОРОВЬЯ НАСЕЛЕНИЯ КЕМЕРОВСКОЙ ОБЛАСТИ

ПРИКАЗ

от 2 июля 2013 г. N 909

ОБ УТВЕРЖДЕНИИ ПРАВИЛ ОСУЩЕСТВЛЕНИЯ ВНУТРЕННЕГО КОНТРОЛЯ СООТВЕТСТВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ ТРЕБОВАНИЯМ К ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ, УСТАНОВЛЕННЫХ ФЕДЕРАЛЬНЫМ ЗАКОНОМ ОТ 27 ИЮЛЯ 2006 ГОДА N 152-ФЗ "О ПЕРСОНАЛЬНЫХ ДАННЫХ" И ПРИНЯТЫМИ В СООТВЕТСТВИИ С НИМ НОРМАТИВНЫМИ ПРАВОВЫМИ АКТАМИ И ЛОКАЛЬНЫМИ АКТАМИ ДЕПАРТАМЕНТА ОХРАНЫ ЗДОРОВЬЯ НАСЕЛЕНИЯ КЕМЕРОВСКОЙ ОБЛАСТИ

Во исполнение Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных", постановления Коллегии Администрации Кемеровской области от 14.03.2007 N 68 "Об утверждении Положения о департаменте охраны здоровья населения Кемеровской области", иных нормативных правовых актов, в целях осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленных федеральным законодательством, а также локальными актами департамента охраны здоровья населения Кемеровской области, приказываю:

1. Утвердить прилагаемые правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленных Федеральным законом от 27 июля 2006 года N 152-ФЗ "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами и локальными актами департамента охраны здоровья населения Кемеровской области.

2. Ознакомить лиц, осуществляющих операции с использованием персональных данных в департаменте охраны здоровья населения Кемеровской области с утвержденными настоящим приказом правилами.

3. Назначить ответственного за организацию обработки персональных данных Гайворонского Д.В.

4. Контроль за исполнением приказа оставляю за собой.

И.о. начальника департамента

О.В.СЕЛЕДЦОВА

Приложение
к приказу
департамента охраны
здоровья населения
Кемеровской области
от 2 июля 2013 г. N 909

ПРАВИЛА
ОСУЩЕСТВЛЕНИЯ ВНУТРЕННЕГО КОНТРОЛЯ СООТВЕТСТВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ ТРЕБОВАНИЯМ К ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ, УСТАНОВЛЕННЫМ ФЕДЕРАЛЬНЫМ ЗАКОНОМ ОТ 27 ИЮЛЯ 2006 Г. N 152-ФЗ "О ПЕРСОНАЛЬНЫХ ДАННЫХ" И ПРИНЯТЫМИ В СООТВЕТСТВИИ С НИМ НОРМАТИВНЫМИ ПРАВОВЫМИ АКТАМИ И ЛОКАЛЬНЫМИ АКТАМИ ДЕПАРТАМЕНТА ОХРАНЫ ЗДОРОВЬЯ НАСЕЛЕНИЯ КЕМЕРОВСКОЙ ОБЛАСТИ

1. Общие положения

1.1. Настоящие правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами и локальными актами департамента охраны здоровья населения Кемеровской области (далее - Правила) разработаны с учетом Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных" и постановления Правительства Российской Федерации от 21 марта 2012 г. N 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, операторами, являющимися государственными или муниципальными органами".

1.2. Настоящие Правила определяют порядок осуществления внутреннего контроля соответствия обработки персональных данных в департаменте охраны здоровья населения Кемеровской области (далее - ДОЗНКО) требованиям к защите персональных данных и действуют постоянно.

2. Тематика внутреннего контроля

1.3. Тематика проверок обработки персональных данных с использованием средств автоматизации.

1.3.1. Соблюдение пользователями информационных систем персональных данных ДОЗНКО парольной политики:

1.3.1.1. Правил формирования пароля;

1.3.1.2. Правил ввода пароля;

1.3.1.3. Правил хранение пароля.

1.3.2. Соблюдение пользователями информационных систем персональных данных ДОЗНКО антивирусной политики:

2.1.2.1. поддержка рабочего состояния антивирусного программного обеспечения;

2.1.2.2. своевременное обновление антивирусного программного обеспечения.

2.1.3. Соблюдение пользователями информационных систем персональных данных ДОЗНКО Правил работы со съемными носителями персональных данных:

2.1.3.1. хранение съемных носителей в персональных шкафчиках пользователей, запирающихся на ключ, расположенных в кабинетах, доступ к которым ограничен соответствующим приказом ДОЗНКО;

2.1.3.2. проверка съемного носителя на наличие вредоносных программ, перед каждым началом работы с ним;

2.1.3.3. исключение копирования с данного носителя файлов сомнительного содержания, и установку нелицензионного программного обеспечения;

2.1.3.4. исключение передачи съемного носителя третьим лицам;

2.1.3.5. запрет на оставление съемного носителя включенным/выключенным без присмотра;

2.1.3.6. запрет на обработку информации, содержащейся на съемном носителе в присутствии третьих лиц;

2.1.3.7. запрет на вынос съемного носителя за пределы служебного помещения.

2.1.4. Соблюдение ответственными за криптографические средства защиты информации Правил работы с ними:

2.1.4.1. хранение криптографических средств в персональных шкафчиках пользователей, запирающихся на ключ, расположенных в кабинетах, доступ к которым ограничен соответствующим приказом ДОЗНКО;

2.1.4.2. исключение передачи криптографического средства третьим лицам;

2.1.4.3. запрет на оставление криптографического средства включенным/выключенным без присмотра;

2.1.4.4. запрет на вынос криптографического средства за пределы служебного помещения;

2.1.4.5. запрет на использование для электронной цифровой подписи открытые и закрытые ключи электронной цифровой подписи, если пользователю известно, что эти ключи используются или использовались ранее;

2.1.4.6. запрет на разглашение конфиденциальной информации, к которой пользователи допущены, средства ее защиты, в том числе сведения о криптографических средствах;

2.1.4.7. обязанность сообщать в орган криптографической защиты о ставших пользователям известными попытках третьих лиц получить сведения об используемых криптографических средствах;

2.1.4.8. обязанность немедленно уведомлять орган криптографической защиты о фактах утраты криптографического средства.

2.1.5. Соблюдение порядка доступа в ДОЗНКО, где расположены элементы

информационных систем персональных данных:

2.1.5.1. все элементы информационных систем хранятся в индивидуальных ящиках, каждого пользователя, запирающихся на ключ, расположенных в кабинетах;

2.1.5.2. соблюдение установленного соответствующего приказа ДОЗНКО ограничения в кабинеты, где используются элементы информационных систем.

2.1.6. Соблюдение порядка резервирования баз данных и хранения резервных копий:

2.1.6.1. наличие актуальных резервных копий;

2.1.6.2. поддержка рабочего состояния систем хранения резервных копий.

2.1.7. Знание пользователей информационных систем персональных данных алгоритма действий во внештатных ситуациях:

2.1.7.1. проведение анкетирования/опроса пользователя о порядке действий во внештатных ситуациях.

2.2. Тематика проверок обработки персональных данных без использования средств автоматизации.

2.2.1. Хранение бумажных носителей с персональными данными:

2.2.1.1. соблюдение хранения бумажные носители, содержащих персональные данные, в закрываемых шкафах;

2.2.1.2. запрет передачи бумажных носителей, содержащих персональные данные третьим лицам;

2.2.1.3. запрет выноса бумажных носителей, содержащих персональные данные за пределы служебного помещения;

2.2.2. Доступ к бумажным носителям с персональными данными:

2.2.2.1. исключение возможности доступа к бумажным носителям, содержащих персональные данные третьих лиц.

2.2.3. Доступ в помещения, где обрабатываются и хранятся бумажные носители с персональными данными:

2.2.3.1. все бумажные носители хранятся в индивидуальных ящиках, каждого пользователя, расположенных в кабинетах;

2.2.3.2. соблюдение установленного соответствующего приказа ДОЗНКО ограничения в кабинеты, где хранятся бумажные носители персональных данных.

3. Порядок проведения проверок условий обработки персональных данных

3.1. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям ДОЗНКО организует раза в три месяца. План проверки утверждается начальником ДОЗНКО (приложение N 1).

3.2. Проверки проводятся по необходимости в соответствии с поручением начальника ДОЗНКО.

3.3. Проверки осуществляются комиссией, образуемой приказом департамента.

3.4. Проверки осуществляются непосредственно на месте обработки персональных

данных путем опроса либо, при необходимости, путем осмотра рабочих мест сотрудников, участвующих в процессе обработки персональных данных.

3.5. Результаты каждой проверки заносятся в протокол (приложение N 2). Протокол подписывается всеми членами комиссии.

3.6. При выявлении в ходе проверки нарушений, в протоколе делается запись о мероприятиях по устранению нарушений и сроках исполнения.

3.7. Протоколы хранятся у ответственного за организацию обработки персональных данных в ДОЗНКО.

3.8. Ответственный за организацию обработки персональных данных докладывает начальнику ДОЗНКО о результатах проверки и мерах, необходимых для устранения нарушений.

4. Права и обязанности комиссии при проведении проверки

4.1. При проведении проверки председатель комиссии:

4.1.1. осуществляет руководство членами комиссии, а также распределяет между ними обязанности;

4.1.2. устанавливает порядок работы комиссии при проведении проверки;

дает членам комиссии указания, обязательные для исполнения;

4.1.3. взаимодействует с должностными лицами ДОЗНКО;

4.1.4. обеспечивает сохранность и возврат полученных оригиналов документов;

4.1.5. обеспечивает соблюдение членами комиссии установленного режима работы и условий функционирования;

4.1.6. докладывает руководству ДОЗНКО о выявленных фактах грубого нарушения законодательства и иных нормативных правовых актов в сфере защиты персональных данных, а также иных обстоятельствах, требующих немедленного реагирования;

4.1.7. отстраняет от участия в работе комиссии ее членов, недобросовестно относящихся к исполнению возложенных на них обязанностей либо допускающих в процессе проверки нарушения служебной дисциплины, о чем немедленно информирует руководство ДОЗНКО;

4.1.8. отчитывается перед начальником ДОЗНКО о ходе и результатах проведения проверки, о работе членов комиссии, об итогах работы по устранению выявленных комиссией нарушений и недостатков;

4.1.9. несет персональную ответственность за качество организации, подготовки и проведения проверки, объективность и обоснованность ее результатов, выводов и предложений, за осуществление контроля по устранению выявленных комиссией нарушений и недостатков в ходе проверки.

4.2. В случае отсутствия председателя его функции и полномочия в полном объеме выполняет заместитель председателя комиссии.

4.3. В рамках проверки председатель (проверяющий), члены комиссии имеют право:

4.3.1. доступа в кабинеты, при предъявлении соответствующего приказа ДОЗНКО;

4.3.2. требовать и получать все необходимые для достижения целей проверки документы (письменные объяснения и иные материалы);

4.3.3. требовать и получать устные разъяснения по существу проверяемых вопросов;

4.3.4. наблюдать за осуществлением деятельности сотрудников ДОЗНКО, с использованием персональных данных;

4.3.5. осуществлять при необходимости анкетирование сотрудников ДОЗНКО, осуществляющих операции с использованием персональных данных;

4.3.6. выполнять иные функции, предусмотренные приказом о проведении проверки.

4.4. Члены комиссии обязаны выполнять распоряжения председателя комиссии.

4.4.1. Члены комиссии несут ответственность:

4.4.1.1. за объективность, полноту и обоснованность сделанных ими в ходе проверки выводов и предложений;

4.4.1.2. за сокрытие выявленных в ходе проверки нарушений законодательства Российской Федерации, а также иных нормативных правовых актов в сфере защиты персональных данных;

4.4.1.3. за превышение в ходе проверки полномочий, предусмотренных настоящими Правилами, а также соответствующим приказом ДОЗНКО о проведении проверки.

Приложение N 1
к Правилам осуществления
внутреннего контроля
соответствия обработки
персональных данных
требованиям к защите
персональных данных,
установленным Федеральным
законом от 27 июля 2006 г.
N 152-ФЗ "О персональных
данных" и принятыми
в соответствии с ним
нормативными правовыми
актами и локальными
актами департамента охраны
здоровья населения
Кемеровской области

План
внутренних проверок условий обработки персональных данных
департамента охраны здоровья населения

N	Тема проверки	Нормативный документ, предъявляющий требования	Срок проведения	Исполнитель
1	2	3	4	5
1	Соблюдение пользователями ИСПДн парольной политики	Инструкция пользователя ИСПДн, разработанная во исполнение приказа ДОЗНКО "О проведении работ по защите персональных данных"		
2	Соблюдение пользователями ИСПДн антивирусной политики			

3	Соблюдение пользователями ИСПДн Правил работы со съемными носителями, на которых содержится информация о персональных данных	от 17.07.2012 N 976		
4	Соблюдение пользователем Правил работы с криптографическими средствами защиты информации	Инструкция пользователя ИСПДн, разработанная во исполнение приказа ДОЗНКО "О проведении работ по защите персональных данных" от 17.07.2012 N 976		
5	Соблюдение порядка доступа в помещения, в которых расположены элементы ИСПДн	Приказ ДОЗНКО "Об ограничении доступа к персональным данным" от 23.03.2012 N 328 (в ред. приказа от 02.07.2013)		
6	Соблюдение порядка резервирования баз данных и хранения резервных копий	Инструкция администратора ИСПДн, разработанная во исполнение приказа ДОЗНКО "О проведении работ по защите персональных данных" от 17.07.2012 N 976		
7	Знание пользователями ИСПДн об алгоритма своих действий во внештатных ситуациях	Инструкция пользователя ИСПДн, разработанная во исполнение приказа ДОЗНКО "О проведении работ по защите персональных данных" от 17.07.2012 N 976		

8	Соблюдение условий хранения бумажных носителей, содержащих информацию о персональных данных	Приказ ДОЗНКО "Об организации работы по защите конфиденциальной информации" от 23.03.12 N 328, приказ ДОЗНКО "Об ограничении доступа к персональным данным"		
9	Соблюдение условий доступа к бумажным носителям, содержащих информацию о персональных данных			
10	Соблюдение условий доступа в помещения, где обрабатываются и хранятся бумажные носители, содержащие информацию о персональных данных	От 23.03.2012 N 328 (в ред. приказа от 02.07.2013)		

Должность ответственного _____ И.О.Фамилия

либо

Председатель комиссии _____ И.О.Фамилия
Председатель комиссии _____ И.О.Фамилия

Приложение N 2
к Правилам осуществления
внутреннего контроля
соответствия обработки
персональных данных
требованиям к защите
персональных данных,
установленным Федеральным
законом от 27 июля 2006 г.
N 152-ФЗ "О персональных
данных" и принятыми
в соответствии с ним
нормативными правовыми
актами и локальными
актами департамента охраны
здоровья населения
Кемеровской области

Протокол
проведения внутренней проверки условий обработки
персональных данных департамента охраны здоровья
населения Кемеровской области

Настоящий Протокол составлен в том, что __.__.201_ ответственным за организацию обработки персональных данных/комиссией по внутреннему контролю проведена проверка
_____.
тема проверки

Проверка осуществлялась в соответствии с требованиями
_____
_____.
название документа

В ходе проверки проверено:
_____
_____
_____
_____
_____
_____.

Выявленные нарушения:
_____
_____
_____
_____

_____
_____
_____.

Меры по устранению нарушений:

_____
_____
_____
_____
_____
_____
_____.

Срок устранения нарушений:

_____.

Должность Ответственного _____ И.О.Фамилия
Председатель комиссии _____ И.О.Фамилия
Члены комиссии:
Должность _____ И.О.Фамилия
Должность _____ И.О.Фамилия
Должность _____ И.О.Фамилия
Начальник ДОЗНКО _____ И.О.Фамилия