ПРАВИЛА
ОСУЩЕСТВЛЕНИЯ ВНУТРЕННЕГО КОНТРОЛЯ СООТВЕТСТВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ ТРЕБОВАНИЯМ К ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

2020 год

Содержание

1. Термины и определения....3
2. Общие положения....4
3. Цели осуществления внутреннего контроля....4
4. Организация внутреннего контроля....5
5. Функции лиц, проводящих внутреннюю проверку....5
6. Мероприятия, проводимые при осуществлении внутреннего контроля....6
7. Способы (методы) осуществления проверок....6
8. Права лиц, осуществляющих внутреннюю проверку....7
9. Обязанности лиц, осуществляющих внутреннюю проверку....7
10. Порядок и сроки предоставления отчёта по проведённой внутренней проверке....7
11. Порядок и сроки устранения выявленных недочётов и нарушений....7
12. Ответственность лиц, проводящих внутреннюю проверку....8

1. Термины и определения

Персональные данные - любая информация, относящаяся к прямо или косвенно определённому или определяемому физическому лицу (субъекту персональных данных).

Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Конфиденциальность персональных данных – обязательное для соблюдения Оператором требование не допускать распространения персональных данных без согласия субъекта персональных данных или наличия иного законного основания.

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Оператор персональных данных – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными. В рамках настоящих Правил Оператором является Администрация городского округа Электросталь Московской области (далее – Оператор).

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределённому кругу лиц.

Сотрудник (работник) – физическое лицо, состоящее в трудовых отношениях с Оператором.

Субъект – физическое лицо, обладатель собственных персональных данных.

Уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

2. Общие положения

2.1 Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее - Правила) определяют порядок организации и осуществления внутреннего контроля в Администрации городского округа Электросталь Московской области.

2.2 Правила разработаны в соответствии с частью 1 статьи 23, статьей 24 Конституции Российской Федерации, главы 14 Трудового кодекса Российской Федерации, Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», постановлением Правительства Российской Федерации от 21.03.2012 № 211, Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

2.3 Настоящие Правила утверждают и вводятся в действие распоряжением главы Администрации городского округа Электросталь Московской области и являются обязательными для исполнения всеми сотрудниками, имеющими доступ к персональным данным.

2.4 Контроль за выполнением требований к защите персональных данных при их обработке в информационных системах персональных данных Администрации городского округа Электросталь Московской области организуется и проводится самостоятельно и (или) с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации. Указанный контроль проводится один раз в три года.

2.5 Настоящие Правила вступают в силу с момента их утверждения распоряжением главы Администрации городского округа Электросталь Московской области и действуют бессрочно.

2.6 Действие настоящих Правил может быть отменено распоряжением главы Администрации городского округа Электросталь Московской области в связи с утратой актуальности, либо по иным причинам.

2.7 Все изменения настоящих Правил утверждаются распоряжением главы Администрации городского округа Электросталь Московской области.

2.8 Все сотрудники Администрации городского округа Электросталь Московской области, допущенные к обработке персональных данных, должны быть ознакомлены с настоящими Правилами под роспись в течение одного месяца с момента принятия настоящих Правил, а также, в аналогичный срок с момента принятия изменений, вносимых в настоящие Правила.

2.9 Все вновь принимаемые на работу в Администрацию городского округа Электросталь Московской области сотрудники, для исполнения должностных обязанностей которых необходим допуск к обработке персональных данных, должны быть ознакомлены (под роспись) с настоящими Правилами до начала исполнения этих обязанностей.

3. Цели осуществления внутреннего контроля

3.1 Целью организации и осуществления внутреннего контроля в Администрации городского округа Электросталь Московской области является соблюдение требований федеральных законов, регулирующих обработку персональных данных в том числе:

а. предотвращение нарушений, связанных с обработкой персональных данных;
б. выполнение установленных законодательными актами Российской Федерации требований к защите персональных данных;

в. выполнение внутренних документов Администрации городского округа Электросталь Московской области, регулирующих обработку персональных данных;
г. выполнение установленных законодательными актами Российской Федерации требований по настройке средств защиты информации;
д. соблюдение правил разграничения прав доступа к информации, содержащей персональные данные;
е. контроль защищённости ИСПДн;
ж. контроль за соблюдением режима обработки персональных данных;
з. контроль за выполнение антивирусной защиты;
и. выявление изменений в режиме обработки и защиты ПДн;
к. выполнение контроля обновления программного обеспечения;
л. контроль за обеспечением резервного копирования;
м. контроль актуальности нормативно-организационных документов.

4. Организация внутреннего контроля

4.1. Функцию контроля в Администрации городского округа Электросталь Московской области выполняют:

а. лицо, ответственное за обработку персональных данных. Данный сотрудник проводит проверку по следующим направлениям: поддержание в актуальном состоянии нормативно-организационных документов, проведение проверок на предмет выявления изменений в режиме обработки и защиты ПДн, повышение квалификации сотрудников в области защиты персональных данных;
б. администратор информационной системы персональных данных. Данный сотрудник проводит проверку по следующим направлениям: управление правами доступа к персональным данным, контроль за обновлениями программного обеспечения;
в. администратор безопасности информационной системы персональных данных. Данный сотрудник проводит проверку по следующим направлениям: контроль прав доступа к персональным данным, контроль защищённости ИСПДн, контроль над соблюдением режима обработки ПДн, контроль над выполнением антивирусной защиты, контроль над функционированием и правильностью настройки средств защиты информации;

4.2. Лицо, ответственное за обработку информации содержащей персональные данные, администратор информационной системы персональных данных, администратор безопасности информационной системы персональных данных назначаются распоряжением главы Администрации городского округа Электросталь Московской области .

5. Функции лиц, проводящих внутреннюю проверку

5.1. В соответствии с поставленными целями, лица, проводящие внутреннюю проверку, осуществляют следующие функции:

5.1.1. Обеспечивают соблюдение выполнения настоящих Правил;

5.1.2. Контролируют соблюдение сотрудниками Администрации городского округа Электросталь Московской области требований федеральных законов, регулирующих обработку персональных данных, в том числе:

а. достоверность представляемой информации о деятельности Администрации городского округа Электросталь Московской области уполномоченному органу по защите прав субъектов персональных данных;
б. соблюдение правил обработки информации, содержащей персональные данные;
в. соблюдение порядка и сроков ответов на запросы субъектов персональных данных;
г. соответствие правильного и своевременного ведения журналов, утверждённых Оператором;
д. исполнение предписаний уполномоченного органа по защите персональных данных;
е. соблюдение мер, направленных на предотвращение распространения персональных данных;
ж. соответствие договоров, заключённых Администрацией городского округа Электросталь Московской области с организациями, предоставляющими услуги Оператору, требованиям федеральных законов, регулирующих обработку персональных данных в том числе.

5.1.3. Взаимодействуют с сотрудниками уполномоченного органа по защите персональных данных, а также с организациями, работающими совместно с Администрацией городского округа Электросталь Московской области, по вопросам обработки персональных данных.

5.1.4. Рассматривают поступающие в адрес Администрации городского округа Электросталь Московской области запросы от субъектов персональных данных, связанных с осуществлением Администрацией городского округа Электросталь Московской области обработки персональных данных субъекта.

5.1.5. Контролируют устранение выявленных нарушений в области обработки персональных данных и соблюдение мер по предупреждению аналогичных нарушений в дальнейшем.

5.1.6. Представляют главе Администрации городского округа Электросталь Московской области по проведённым внутренним проверкам.

5.1.7. Осуществляют в соответствии с внутренними документами Администрации городского округа Электросталь Московской области и законодательными актами РФ иные функции по контролю за соблюдением сотрудниками Администрации городского округа Электросталь Московской области законодательства Российской Федерации, регулирующего обработку персональных данных.

6. Мероприятия, проводимые при осуществлении внутреннего контроля

6.1. При исполнении своих функций лица, проводящие внутреннюю проверку, осуществляют мероприятия согласно ежегодному плану мероприятий по защите персональных данных, утвержденному распоряжением главы Администрации городского округа Электросталь Московской области.

7. Способы (методы) осуществления проверок

7.1. С учётом целей и задач проверки, характера проверяемой деятельности лица, ответственные за проведение внутренней проверки, вправе самостоятельно определять способы (методы) осуществления проверок.

7.2. Основными способами (методами) осуществления проверок являются:
а. проверка актуальности документации, связанной с обработкой персональных данных;
б. проверка соблюдения законодательных актов РФ и внутренних документов, регулирующих обработку персональных данных;

в. операционная проверка, цель которой заключается в оценке соответствия систем, процессов и их достаточности для выполнения функций, связанных с обработкой и защитой персональных данных.

8. Права лиц, осуществляющих внутреннюю проверку

8.1. Лица, осуществляющие внутреннюю проверку, имеют право:

а. принимать участие в работах по разработке внутренних документов Администрации городского округа Электросталь Московской области, связанных с обработкой персональных данных;

б. получать доступ к необходимой для осуществления проверки правовой и нормативной документации, а также к локальным нормативным актам и документации по обеспечению безопасности персональных данных.

9. Обязанности лиц, осуществляющих внутреннюю проверку

9.1. Лица, осуществляющие внутреннюю проверку обязаны:

а. соблюдать требования федеральных законов и иных нормативных правовых актов РФ;

б. соблюдать правила внутреннего контроля Администрации городского округа Электросталь Московской области;

в. инициировать разбирательства по фактам несоблюдения условий обработки персональных данных;

г. проводить разъяснительную работу с сотрудниками Администрации городского округа Электросталь Московской области по вопросам, связанным с осуществлением внутреннего контроля;

д. информировать о выявленных при проведении проверок нарушениях или недостатках главу Администрации городского округа Электросталь Московской области.

10. Порядок и сроки предоставления отчёта по проведённой внутренней проверке

10.1. По результатам внутренней проверки лица, ответственные за её проведение, в срок не превышающий 10 рабочих дней с даты окончания проверки, предоставляют отчёт главе Администрации городского округа Электросталь Московской области.

10.2. Отчёт должен содержать:

а. описание целей проверки;

б. сроки проведения проверки;

в. перечень проведённых мероприятий;

г. перечень выявленных нарушений и недочётов;

д. рекомендации по устранению выявленных нарушений.

10.3. Все экземпляры отчётов о проверке, представленные главе Администрации городского округа Электросталь Московской области, возвращаются лицам, ответственным за проведение проверки, с пометкой, свидетельствующей об ознакомлении с отчётом.

11. Порядок и сроки устранения выявленных недочётов и нарушений

11.1. Глава Администрации городского округа Электросталь Московской области организует в течение 10 рабочих дней со дня получения отчёта о проверке, в котором зафиксированы нарушения, разработку плана мероприятий по проведению работ в целях устранения и недопущения в дальнейшем выявленных в ходе проверки нарушений и недочётов.

11.2. План мероприятий должен содержать конкретные действия по устранению и дальнейшему недопущению нарушений и замечаний, указанных в отчёте о проверке, сроки и ответственных за их выполнение.

11.3. План мероприятий утверждается распоряжением главы Администрации городского округа Электросталь Московской области.

11.4. В целях осуществления контроля информация об устранении недостатков и мерах, принятых по итогам рассмотрения результатов проверки, с приложением плана мероприятий по проведению работ в целях устранения и недопущения в дальнейшем выявленных в ходе проверки нарушений и недочётов представляется проверенным структурным подразделением в срок не позднее 15 рабочих дней с момента получения отчёта.

12. Ответственность лиц, проводящих внутреннюю проверку

12.1. Ответственные лица, осуществляющие проведение внутренней проверки, несут ответственность за:

а. за неисполнение (ненадлежащее исполнение) своих обязанностей, предусмотренных настоящими Правилами и должностными инструкциями ответственных лиц.

б. за совершенные в процессе осуществления своей деятельности правонарушения – в пределах, определённых действующим административным, уголовным и гражданским законодательством Российской Федерации.