|  |
| --- |
| ПРИЛОЖЕНИЕ №6УТВЕРЖДЕНОРаспоряжением «О вводе в действие комплекта организационно-распорядительной документации по организации обработки и защиты персональных данных» администрации МР «Куйбышевский район»от «19» ноября 2020 г. № 408-р (М.П.) |

|  |
| --- |
| **Правила**осуществления внутреннего контроля обработки персональных данных на соответствие требованиям к их защите |

Оглавление

[1. Общие положения. 3](#_Toc479002645)

[2. Основание проведения контроля и сроки. 3](#_Toc479002646)

[3. Контроль выполнения требований постановления Правительства №1119. 4](#_Toc479002647)

[4. Заключительные положения. 5](#_Toc479002648)

[Приложение №1. 7](#_Toc479002649)

1. **Общие положения.**
	1. Настоящие правила определяют основания, форму и порядок осуществления в администрации (исполнительно-распорядительного органа) муниципального района «Куйбышевский район» Калужской области (далее – Администрация МР «Куйбышевский район») внутреннего контроля на соответствие обработки персональных данных (далее – ПДн) в информационных системах персональных данных (далее – ИСПДн) «Экономика», «Бухгалтерия и кадры», «ЖКХ», «Комиссия по делам несовершеннолетних» требованиям к защите ПДн и политике в отношении обработки ПДн.
	2. Настоящие правила разработаны в соответствии:
		1. с Федеральным законом Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ);
		2. с постановлением Правительства Российской Федерации от 01 января 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» (далее – постановление Правительства № 1119);
		3. с постановлением Правительства РФ от 21 марта 2012 года № 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».
	3. Основные понятия и термины, используемые в настоящих правилах, применяются в значениях, определенных статьей 3 Федерального закона № 152-ФЗ.
2. **Основание проведения контроля и сроки.**
	1. Основанием для проведения внутреннего контроля являются требования части 1, статьи 18.1 Федерального закона № 152-ФЗ, пункта 17 постановления Правительства № 1119, пункта д) части 1 постановления Правительства № 211.
	2. Внутренний контроль осуществляется путем проведения периодических проверок и контроля выполнения требований постановления Правительства № 1119 **не реже 1 раза в год**.
3. **Контроль выполнения требований постановления Правительства
№ 1119.**
	1. Контроль выполнения требований постановления Правительства № 1119 проводит Комиссия, назначенная распоряжением руководителя Администрации МР «Куйбышевский район».
	2. Состав Комиссии не менее 3-х человек, включая ответственного за организацию обработки ПДн. Все члены комиссии при принятии решения обладают равными правами.
	3. Комиссия при проведении проверки обязана:
		1. провести анализ реализации мер, направленных на обеспечение выполнения Администрацией МР «Куйбышевский район» обязанностей, предусмотренных статьями 18.1, 19 Федерального закона № 152-ФЗ и принятыми в соответствии с ним локальными актами в отношении обработки ПДн в каждой ИСПДн;
		2. провести анализ выполнения Администрацией МР «Куйбышевский район» требований по определению и обеспечению уровня защищенности ПДн, утвержденных постановлением Правительства № 1119 для каждой ИСПДн в отдельности;
		3. провести анализ условий обработки ПДн, проверку утвержденных документов, регулирующих порядок обработки ПДн, установленных постановлением Правительства № 211;
		4. провести анализ реализации Администрацией МР «Куйбышевский район» организационных и технических мер по обеспечению безопасности ПДн, утвержденных распоряжением ФСТЭК России от 18 февраля 2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
		5. провести анализ состава оборудования, программных средств, включая средства защиты, входящих в состав ИСПДн на соответствие техническим паспортам ИСПДн;
		6. своевременно и в полной мере исполнять предоставленные полномочия по предупреждению, выявлению и пресечению нарушений требований к защите ПДн, установленных законодательными и нормативными правовыми актами Российской Федерации;
	4. Комиссия при проведении проверки вправе:
		1. запрашивать и получать необходимые документы (сведения) для достижения целей проведения внутреннего контроля;
		2. получать временный доступ к ресурсам ИСПДн в части касающейся ее полномочий;
		3. принимать меры по приостановлению или прекращению обработки ПДн, осуществляемой с нарушением требований к защите ПДн;
		4. вносить руководителю Администрации МР «Куйбышевский район» предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении требований к защите ПДн, установленных законодательными и нормативными правовыми актами Российской Федерации.
	5. При проведении проверки члены Комиссии не вправе:
		1. требовать представления документов и сведений, не относящихся к предмету проверки;
		2. распространять информацию и сведения конфиденциального характера, полученные при проведении проверки.
	6. По результатам проверки составляется Акт проверки, который подписывается членами комиссии и представляется руководителю Администрации МР «Куйбышевский район» для принятия соответствующего решения. В Администрации МР «Куйбышевский район» разработана и используется специальная форма соответствующего Акта (**Приложение №1**).
	7. В Акте отражаются сведения о результатах проверки, в том числе о выявленных нарушениях обязательных требований законодательных и нормативных правовых актов Российской Федерации в области защиты ПДн, об их характере и о лицах, допустивших указанные нарушения.
	8. Акт должен содержать заключение о соответствии или несоответствии обработки ПДн требованиям к защите ПДн и политике Администрации МР «Куйбышевский район» в отношении обработки ПДн, установленным Федеральным законом Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами. Заключение о соответствии должно быть сформулировано для каждой из ИСПДн в отдельности.
4. **Заключительные положения.**
	1. Пользователи ИСПДн, участвующие в обработке ПДн, должны ознакомиться с настоящими правилами проведения внутреннего контроля.
	2. Обязанность доводить до сведения работников Администрации МР «Куйбышевский район» правила внутреннего контроля лежит на ответственном за организацию обработки ПДн.
	3. Сотрудники Администрации МР «Куйбышевский район», несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящими Правилами, в пределах, определенных действующим законодательством Российской Федерации.

**Приложение №1**

**Акт №** \_\_\_\_\_\_\_\_

проведения внутренней проверки условий

обработки персональных данных в администрации (исполнительно-распорядительного органа) муниципального района «Куйбышевский район» Калужской области

Дата составления: «\_\_\_\_» \_\_\_\_\_\_\_ 20\_\_\_\_ г.

Место проведение проверки: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Комиссия, назначенная распоряжением руководителя от «\_\_\_» \_\_\_\_\_\_\_ 20\_\_\_ № \_\_\_\_ в составе:

Председатель:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(Ф.И.О.)

Члены комиссии:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(Ф.И.О.)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(Ф.И.О.)

руководствуясь «Правилами осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, политике администрации (исполнительно-распорядительного органа) муниципального района «Куйбышевский район» Калужской области (далее – Администрация МР «Куйбышевский район») в отношении обработки персональных данных» провела проверку условий обработки персональных данных в Администрации МР «Куйбышевский район».

В ходе проверки:

* проведен анализ реализации мер, направленных на обеспечение выполнения оператором обязанностей, предусмотренных статьями 18.1, 19 Федерального закона Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним локальными актами оператора определяющих его политику в отношении обработки персональных данных;
* проведен анализ условий обработки персональных данных, проверка утвержденных документов, регулирующих порядок обработки персональных данных, установленных постановлением Правительства РФ от 21 марта 2012 года № 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»;
* проведен анализ выполнения оператором требований по определению и обеспечению уровня защищенности персональных данных, утвержденных постановлением Правительства Российской Федерации от 01 января 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
* проведен анализ реализации оператором организационных и технических мер по обеспечению безопасности персональных данных, утвержденных распоряжением ФСТЭК России от 18 февраля 2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
* проведен анализ состава оборудования, программных средств, включая средства защиты, входящих в состав информационной системы персональных данных на соответствие Техническому паспорту информационной системы.

Выявленные нарушения: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

ЗАКЛЮЧЕНИЕ комиссии:

Обработка персональных данных соответствует (не соответствует) *(нужное подчеркнуть*) требованиям к защите персональных данных и политике организации в отношении обработки персональных данных, установленным Федеральным законом Российской Федерации от 27 июля 2006 № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами.

Председатель комиссии: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (подпись)

Члены комиссии: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (подпись)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (подпись)