АДМИНИСТРАЦИЯ ГОРОДСКОГО ОКРУГА ТОЛЬЯТТИ

РАСПОРЯЖЕНИЕ

03.06.2024 № 4673-р/1

г. Тольятти, Самарской области

О внесении
изменений в распоряжение мэрии городского
округа Тольятти от 12.07.2013 № 4292-р/1
«Об утверждении Правил осуществления
внутреннего контроля соответствия обработки
персональных данных требованиям к защите
персональных данных, установленных
Федеральным законом “О персональных данных”,
принятыми в соответствии с ним нормативными
правовыми актами и муниципальными правовыми
актами в мэрии городского округа Тольятти»

В целях совершенствования муниципального правового акта, руководствуясь Уставом городского округа Тольятти,

1. Внести в распоряжение мэрии городского округа Тольятти от 12.07.2013 № 4292-р/1 «Об утверждении Правил осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленных Федеральным законом “О персональных данных”, принятыми в соответствии с ним нормативными правовыми актами и муниципальными правовыми актами в мэрии городского округа Тольятти» (далее – распоряжение, Правила) следующие изменения:

1.1. В наименовании, преамбуле, пунктах 1,2,3 распоряжения слово «мэрии» заменить словом «администрации».

2. Внести в Правила следующие изменения:

2.1. В наименовании, абзаце втором раздела I, абзаце первом пункта 1.1 раздела I Правил слово «мэрии» заменить словом «администрации».

2.2. Абзац первый раздела II Правил изложить в следующей редакции:

«2.1. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям в администрации организуется проведение периодических проверок условий обработки персональных данных.».

2.3. Пункт 2.2. раздела II Правил изложить в следующей редакции:

«2.2. Проверки осуществляются департаментом информационных технологий и связи администрации (далее – ДИТиС). Ответственным за организацию проверок является сотрудник, ответственный за организацию обработки персональных данных.».

2.4. Абзац первый пункта 2.3 раздела II Правил изложить в следующей редакции:

«2.3. Плановые проверки соответствия обработки персональных данных установленным требованиям в администрации проводятся на основании утвержденного приказом руководителя ДИТиС ежегодного плана.».

2.5. В пунктах 2.3, 2.4 раздела II Правил слово «мэрии» заменить словом «администрации».

2.6. Пункт 2.5 раздела II Правил изложить в следующей редакции:

«2.5. Ответственный за организацию проверок имеет право:

- запрашивать у сотрудников органов администрации информацию, необходимую для реализации полномочий;

- принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства Российской Федерации;

- вносить руководителю ДИТиС предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке.».

2.7. Пункт 2.8 раздела II Правил изложить в следующей редакции:

«2.8. Ответственный за организацию проверок предоставляет руководителю ДИТиС акт о результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений по форме согласно приложению №1 к настоящим Правилам.».

2.8. В пунктах 3.2, 3.3, 3.8, 3.11 раздела Ш Правил слово «мэрия» заменить словом «администрация» в соответствующем числе и падеже.

2.9. Пункт 3.4 раздела Ш Правил изложить в следующей редакции:

«3.4. Выявление инцидента ИБ.

Основными источниками информации об инцидентах ИБ являются:

- результаты плановых или внеплановых проверок соответствия обработки персональных данных установленным требованиям;
- факты, выявленные сотрудниками органов администрации.

Сотрудник органа администрации может выявить признаки наличия Инцидента ИБ путем анализа текущей ситуации на предмет ее соответствия требованиям распоряжения мэра городского округа Тольятти от 30.12.2010 № 13996-р/1 «Об утверждении Положения об обработке персональных данных в администрации городского округа Тольятти» (далее - Положение об обработке ПДн). Выявленные несоответствия дают основания предполагать факт возникновения инцидента ИБ. Любые сведения о предполагаемом инциденте ИБ незамедлительно передаются выявившим их сотрудником в ДИТиС в произвольной форме любым доступным способом:

- по контактам, указанным в телефонном справочнике официального сайта администрации;
- через непосредственного руководителя.»;

2.10. Пункт 3.5 раздела Ш Правил изложить в следующей редакции:

«3.5. Ответственный за проведение проверок после получения информации о предполагаемом инциденте ИБ незамедлительно фиксирует дату, время и место возникновения предполагаемого инцидента ИБ и определяет сотрудника ДИТиС, осуществляющего разбирательство.».

2.11. Пункт 3.6 раздела Ш Правил изложить в следующей редакции:

«3.6. В срок не более одного рабочего дня с момента поступления информации об инциденте ИБ, сотрудник ДИТиС, осуществляющий разбирательство, определяет и инициирует первоочередные меры (отключение АРМ предполагаемого нарушителя ИБ от информационной системы, восстановление информации из резервной копии, исправление ошибки ввода, проведение дополнительного инструктажа по ИБ), направленные на локализацию инцидента ИБ и минимизацию его последствий.».

2.12. Пункт 3.7 раздела Ш Правил изложить в следующей редакции:

«3.7. В случае нарушения прав субъекта персональных данных разбирательство и реагирование происходит в порядке и в сроки, предусмотренные Правилами рассмотрения запросов субъектов персональных данных в администрации городского округа Тольятти, утвержденными постановлением мэрии от 24.05.2013 № 1670-п/1 «Об утверждении Правил рассмотрения запросов субъектов персональных данных или их представителей в администрации городского округа Тольятти».».

2.13. Подпункт 3.8.2 пункта 3.8 раздела Ш Правил изложить в следующей редакции:

«3.8.2. Осуществляющий разбирательство сотрудник ДИТиС в процессе проведения расследования инцидента ИБ при необходимости запрашивает информацию в органах администрации. Запрос направляется на имя руководителя органа администрации с указанием сроков предоставления информации (с учетом необходимости ее анализа, сбора и подготовки).».

2.14. В подпункте 3.8.3 пункта 3.8 раздела Ш Правил слово «сотрудник» заменить словами «сотрудник ДИТиС».

2.15. В подпункте 3.8.4 пункта 3.8 раздела Ш Правил слово «сотрудником» заменить словами «сотрудником ДИТиС».

2.16. В подпункте 3.8.5 пункта 3.8 раздела Ш Правил слово «сотрудника» заменить словами «сотрудника ДИТиС».

2.17. В пункте 3.10 раздела Ш Правил слово «сотрудником» заменить словами «сотрудником ДИТиС».

2.18. В пункте 3.11 раздела Ш Правил слово «сотрудником» заменить словами «сотрудником ДИТиС».

2.19. Пункт 3.12 раздела Ш Правил изложить в следующей редакции:

«3.12. На основании полученного акта разбирательства инцидента ИБ руководитель органа администрации, затронутого инцидентом ИБ, в срок не более трех рабочих дней организует проведение мероприятий, направленных на снижение рисков ИБ в будущем:

- повторное ознакомление нарушителя ИБ с должностной инструкцией, с действующими нормативно-правовыми актами в области ИБ;
- анализ и пересмотр имеющихся прав доступа к информационным ресурсам у нарушителя ИБ;
- доведение до всех сотрудников органа администрации требований правовых актов в области ИБ.».

3. Приложение № 1 к Правилам изложить в редакции согласно Приложению к настоящему распоряжению.

4. В Приложении № 2 к Правилам слово «мэрии» заменить словом «администрации».

5. В Приложении № 3 к Правилам слово «мэрии» заменить словом «администрации».

6. В Приложении № 3 к Правилам слова «сотрудником отдела информационной безопасности» заменить словами «сотрудником ДИТиС».

7. В Приложении № 3 к Правилам слова «подпись начальника отдела информационной безопасности» заменить словами «подпись ответственного за организацию проверок».

Глава городского округа Н.А.Ренц

Приложение к распоряжению
администрации городского округа Тольятти
от 03.06.2024 № 4673-р/1

Приложение №1
к Правилам осуществления внутреннего
контроля соответствия обработки персональных
данных требованиям к защите персональных
данных, установленным Федеральным Законом
«О персональных данных», принятыми в
соответствии с ним нормативными правовыми
актами и муниципальными правовыми актами
в администрации городского округа Тольятти

Акт проверки соответствия условий обработки персональных данных положению об обработке персональных данных в

_____
(наименование структурного подразделения органа администрации)

_____ _____
Адрес расположения дата

Раздел, пп. Положения	Проверяемое условие обработки ПДн	Отметка о соответствии
II, 2.1.2.	Наличие записи в должностных инструкциях сотрудников	да / нет
	Наличие подписанного обязательства о неразглашении информации, содержащей персональные данные	да / нет
II, 2.2.1.	Наличие согласия субъекта ПДн об обработке ПДн (за исключением случаев, предусмотренных частью 2 статьи 6 Федерального закона от 27.07.2006г. № 152–ФЗ «О персональных данных»)	да / нет / не требуется
II, 2.2.2.	Наличие утвержденного перечня работников подразделения мэрии, допущенных к обработке персональных данных в связи с исполнением своих служебных (трудовых) обязанностей	да / нет
II, 2.2.3.	Отсутствие обработки специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических	да / нет

	взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни	
II, 2.2.6.; II, 2.4.7.	Наличие журнала учета электронных носителей персональных данных	да / нет / не требуется
при автоматизированной обработке ПДн		
II, 2.2.7.	Отсутствие обработки необезличенных ПДн после достижения цели, в случае отсутствия необходимости в достижении цели обработки ПДн, в случае отзыва субъектом персональных данных согласия на обработку	да / нет
II, 2.3.2.	Функционирование на АРМ пользователей системы антивирусной защиты, СЗНСД (при наличии)	да / нет
при неавтоматизированной обработке ПДн		
II, 2.4.2.	Использование отдельных носителей для каждой категории персональных данных	да / нет / не требуется
II, 2.4.3.	Отсутствие фиксации на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы	да / нет
	Обособление ПДн от иной информации, на отдельных материальных носителях, в специальных разделах или на полях форм (бланков)	да / нет
II, 2.4.3.	Группировка документов, содержащих ПДн в отдельные дела (папки) в зависимости от цели их обработки	да / нет
	Наличие внутренних описей документов с указанием цели обработки и категории персональных данных в делах с документами, содержащими ПДн	да / нет / не требуется
II, 2.4.6.	Наличие организационных (охрана помещений) и технических мер (установка сертифицированных средств защиты информации), исключающих возможность несанкционированного доступа к персональным данным лиц, не допущенных к их обработке	да / нет
II, 2.4.10.	Хранение документов и внешних электронных носителей информации, содержащих ПДн в запираемых и опечатываемых металлических шкафах (сейфах).	да / нет / не требуется

II, 2.4.11.	Наличие оформленных актов при уничтожении ПДн	да / нет
III.	Наличие приказа о назначении ответственного за проведение мероприятий по защите персональных данных	да / нет

От ДИТиС:

_____

_____

От структурного подразделения органа администрации:

_____

_____