Приложение №3
к приказу комитета
региональной безопасности
Курской области
от 13.04.2021 № 47

Правила
рассмотрения запросов субъектов персональных данных или их представителей

Общие положения

Настоящие Правила разработаны в соответствии с Федеральным законом от 27 июля 2006 г. №152-ФЗ «О персональных данных» (далее - Федеральный закон №152-ФЗ), Федеральным законом от 2 мая 2006 г. № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации», постановлением Правительства Российской Федерации от 21 марта 2012 г. № 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 и муниципальными органами» и определяют порядок организации работы по приему, регистрации и рассмотрению поступивших в комитет региональной безопасности Курской области (далее Оператор) запросов субъектов персональных данных или их представителей (далее - запросы).

Целью настоящих Правил является упорядочение действий должностных лиц оператора при обращении либо при получении запросов.

Прием, регистрация и рассмотрение запросов

Сведения, касающиеся обработки персональных данных субъекта персональных данных, предоставляются Оператором субъекту персональных данных или его представителю при обращении либо при получении запроса субъекта персональных данных или его представителя.

Запрос может быть подан одним из следующих способов:

лично;

письменно;

с использованием средств факсимильной связи или электронной связи, в том числе через официальный сайт оператора в информационно-телекоммуникационной сети «Интернет».

Информация об Операторе, включая информацию о месте его нахождения, графике работы, контактных телефонах, а также о порядке обработки персональных данных размещается:

на стендах, расположенных в помещениях, занимаемых Оператором;

на официальном сайте Оператора в информационно-телекоммуникационной сети «Интернет» (разделе официального сайта Администрации Курской области).

Прием субъектов персональных данных или их представителей ведется сотрудниками Оператора, ответственными за прием и регистрацию обращений.

При приеме субъект персональных данных или его представитель предъявляет документ, удостоверяющий его личность, а также документ, подтверждающий полномочия представителя (в случае обращения представителя).

Содержание устного обращения заносится в карточку личного приема. В случае если изложенные в устном обращении факты и обстоятельства являются очевидными и не требуют дополнительной проверки, ответ с согласия субъекта персональных данных

или его представителя может быть дан устно в ходе личного приема, о чем делается запись в карточке личного приема. В остальных случаях дается письменный ответ по существу поставленных в обращении вопросов.

В том случае, когда при личном приеме субъект персональных данных или его представитель изъявил желание получить ответ в письменной форме, сотрудник Оператора, ответственный за прием и регистрацию обращений, предлагает оформить письменный запрос и сообщает ему о сроках, в течение которых Оператор обязан дать ответ на такой запрос в соответствии с федеральным законом.

В случае, если в обращении содержатся вопросы, решение которых не входит в компетенцию Оператора, субъекту персональных данных или его представителю дается разъяснение, куда и в каком порядке ему следует обратиться.

Запросы регистрируются в день их поступления к Оператору в Журнале учета обращений субъектов персональных данных.

Днем обращения считается дата регистрации запроса субъекта персональных данных или его представителя.

Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с Оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Оператором, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

Рассмотрение запросов субъектов персональных данных или их представителей осуществляется сотрудниками Оператора, ответственными за их рассмотрение и подготовку ответов (далее - уполномоченные сотрудники оператора).

При рассмотрении запросов обеспечивается:

объективное, всестороннее и своевременное рассмотрения запроса;

принятие мер, направленных на восстановление или защиту нарушенных прав, свобод и законных интересов субъектов персональных данных;

направление письменных ответов по существу запроса.

Запрос прочитывается, проверяется на повторность, при необходимости сверяется с находящейся в архиве предыдущей перепиской.

Оператор вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным частями 4 и 5 статьи 14 Федерального закона № 152-ФЗ. Такой отказ должен быть мотивированным.

Оператор обязан сообщить субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя в течение десяти календарных дней с даты обращения субъекта персональных данных или его представителя.

В случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта персональных данных или его представителя сотрудники Оператора обязаны дать в письменной форме мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 Федерального закона № 152-ФЗ или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий семи рабочих дней со дня обращения субъекта персональных данных или его представителя.

Оператор обязан предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных.

Для проверки фактов, изложенных в запросах при необходимости организуются служебные проверки в соответствии с законодательством.

Запрос считается исполненным, если рассмотрены все поставленные в нем вопросы, приняты необходимые меры и даны исчерпывающие ответы.

Контроль за соблюдением порядка рассмотрения запросов субъектов персональных данных или их представителей.

Оператор осуществляет контроль за соблюдением установленного законодательством и настоящими Правилами порядка рассмотрения запросов.

Нарушение установленного порядка рассмотрения запросов влечет в отношении виновных сотрудников оператора ответственность в соответствии с законодательством Российской Федерации.

Уведомление

Уважаемый(ая) _____
(Ф.И.О.)

Комитетом региональной безопасности Курской области производиться обработка сведений, составляющих Ваши персональные данные:

(указать сведения)

Цели обработки:
Способы обработки:
Перечень лиц, которые имеют доступ к информации, содержащей Ваши персональные данные или могут получить такой доступ:

№	Должность	Ф.И.О.	Вид доступа	Примечания

По результатам обработки указанной информации нами планируется принятие следующих решений, которые будут доведены до Вашего сведения.

_____

Против принятого решения Вы имеете право заявить свои письменные возражения в срок.

(должность) _____ (подпись) _____ (ФИО)

«___» _____20__ г.

В комитет
региональной
безопасности
Курской области

от _____
(ф.и.о. заявителя)

_____
(наименование и реквизиты документа,
удостоверяющего личность заявителя)

Заявление

Прошу заблокировать, обрабатываемые Вами, мои персональные данные:

(указать блокируемые персональные данные)

на срок: _____
(указать срок блокирования)

в связи с тем, что _____
(указать причину блокирования персональных данных)

_____ _____
(должность) (ФИО)

(подпись)

«__ »20_____ г.

В комитет
региональной
безопасности
Курской области

от _____
(ф.и.о. заявителя)

(наименование и реквизиты документа,
удостоверяющего личность заявителя)

Заявление

Прошу уничтожить, обрабатываемые Вами, мои персональные данные:

_____;
(указать уничтожаемые персональные данные)

в связи с тем, что _____.
(указать причину уничтожения персональных данных)

_____ _____
(подпись) (ФИО)

« __ »20 _____ г.

В комитет
региональной
безопасности
Курской области

от _____
(ф.и.о. заявителя)

_____
(наименование и
реквизиты документа,
удостоверяющего
личность заявителя)

Заявление

Прошу уточнить, обрабатываемые Вами, мои персональные данные в соответствии со сведениями: _____;

(указать уточненные персональные данные заявителя)

в связи с тем, что _____.

(указать причину уточнения персональных данных)

_____
(ФИО)

(подпись)

«__ »20_____ г.

Лист ознакомления

№ п/п	Ф.И.О.	Роспись
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		
11.		
12.		
13.		
14.		
15.		
16.		
17.		
18.		
19.		
20.		
21.		
22.		
23.		
24.		
25.		
26.		
27.		
28.		

Приложение №4
к приказу комитета
региональной безопасности
Курской области
от 13.04.20___ № 47

ПРАВИЛА
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 локальными актами комитета региональной безопасности Курской области

1. Общие положения

1.1. Настоящие правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее - Правила) в комитете региональной безопасности Курской области (далее - комитет), определяют процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере обработки персональных данных, а также основания, порядок, формы и методы проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.

1.2. Настоящие Правила разработаны на основании Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и в соответствии с частью 1 «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», утвержденных постановлением Правительства Российской Федерации от 21 марта 2012 г. № 211.

1.3. Для обработки персональных данных в комитете используются информационные системы, перечень которых утверждается руководителем комитета (далее - информационные системы).

1.4. Пользователем информационной системы (далее - Пользователь) является работник комитета, участвующий в рамках выполнения своих функциональных обязанностей в процессах автоматизированной обработки персональных данных и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты информации информационной системы.

1.5. Контрольные мероприятия за обеспечением уровня защищенности персональных данных и соблюдений условий использования средств защиты информации, а также соблюдением требований законодательства Российской Федерации по обработке персональных данных в информационных системах проводятся в следующих целях:

1.5.1. проверка выполнения требований организационно-распорядительной документации по защите информации в комитете и действующего законодательства Российской Федерации в области обработки и защиты персональных данных;

1.5.2. оценка уровня осведомленности и знаний работников комитета в области обработки и защиты персональных данных;

1.5.3. оценка обоснованности и эффективности применяемых мер и средств защиты информации.

2. Тематика внутреннего контроля

Тематика внутреннего контроля соответствия обработки персональных данных

требованиям к защите персональных данных:

2.1. Проверки соответствия обработки персональных данных установленным требованиям в комитете разделяются на следующие виды:

2.1.1 регулярные;

2.1.2 плановые;

2.1.3 внеплановые.

2.2. Регулярные контрольные мероприятия проводятся периодически должностным лицом, ответственным за обеспечение безопасности персональных данных в соответствии с требованиями организационно распорядительной документации и предназначены для осуществления контроля выполнения требований в области защиты персональных данных.

2.3. Плановые контрольные мероприятия проводятся периодически в соответствии с утвержденным Планом проведения контрольных мероприятий (далее - План, приложение 1) и направлены на постоянное совершенствование системы защиты персональных данных информационной системы.

2.4. Внеплановые контрольные мероприятия проводятся на основании решения комиссии по информационной безопасности. Решение о проведении внеплановых контрольных мероприятий и созданию комиссии по информационной безопасности может быть принято в следующих случаях:

2.4.1 по результатам расследования инцидента информационной безопасности;

2.4.2 по результатам внешних контрольных мероприятий, проводимых регулирующими органами;

2.4.3 по решению председателя комитета.

3. План проведения контрольных мероприятий

3.1. Для проведения плановых внутренних контрольных мероприятий ответственный за обеспечение безопасности персональных данных в комитете, разрабатывает План внутренних контрольных мероприятий на текущий год.

3.2. План проведения внутренних контрольных мероприятий (как плановых, так и внеплановых) включает следующие сведения по каждому из мероприятий:

3.2.1 цели проведения контрольных мероприятий;

3.2.2 задачи проведения контрольных мероприятий,

3.2.3 объекты контроля (процессы, подразделения, информационные системы и т.п.);

3.2.4 состав участников, привлекаемых для проведения контрольных мероприятий;

3.2.5 сроки и этапы проведения контрольных мероприятий.

3.3. Общий срок контрольных мероприятий не должен превышать пяти рабочих дней. При необходимости срок проведения контрольных мероприятий может быть продлен, но не более чем на десять рабочих дней, соответствующие изменения отображаются в Отчете, выполняемом по результатам проведенных контрольных мероприятий.

4. Оформление результатов проведенных контрольных мероприятий

4.1. По итогам проведения внутренних контрольных мероприятий, ответственный за обеспечение безопасности персональных данных в комитете, разрабатывает отчет, в котором указывается:

4.1.1 описание проведенных мероприятий по каждому из этапов в соответствии

с планом;

4.1.2 отклонения от плана, в случае их наличия;

4.1.3 перечень и описание выявленных нарушений;

4.1.4 рекомендации по устранению выявленных нарушений.

4.1.5 заключение по итогам проведения внутреннего контрольного мероприятия.

4.2. Отчет передается на рассмотрение председателю комитета.

4.3. Общая информация о проведенном контрольном мероприятии фиксируется в Журнале регистрации проверок в сфере защиты персональных данных.

4.4. Результаты проведения мероприятий по плановому и внеплановому контролю заносятся в протокол (акт) проведения внутренних проверок контроля соответствия обработки персональных данных требованиям к защите персональных данных в комитете (приложение 2).

5. Общий порядок проведения контрольных мероприятий

5.1. Контрольные мероприятия проводятся ответственным за обеспечение безопасности обработки персональных данных.

5.2. Ответственный за обеспечение безопасности персональных данных не позднее чем за три рабочих дня до начала проведения контрольных мероприятий уведомляет всех руководителей подразделений, в которых планируется проведение контрольных мероприятий, и направляет им для ознакомления План проведения контрольных мероприятий. При проведении внеплановых контрольных мероприятий уведомление не требуется.

5.3. Во время проведения контрольных мероприятий, в зависимости от целей мероприятий, могут выполняться следующие проверки:

5.3.1 соответствие полномочий Пользователя правилам доступа;

5.3.2 соблюдение Пользователями требований инструкций по организации антивирусной и парольной защите, инструкции по обеспечению безопасности персональных данных;

5.3.3 соблюдение Порядка доступа в помещения, где ведется обработка персональных данных;

5.3.4 порядок и условия применения средств защиты информации;

5.3.5 состояние учета машинных носителей персональных данных;

5.3.6 наличие (отсутствие) фактов несанкционированного доступа к персональных данных и принятие необходимых мер;

5.3.7 проведенные мероприятия по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

5.3.8 технические мероприятия, связанные со штатным и нештатным функционированием средств защиты информации;

5.3.9 технические мероприятия, связанные со штатным и нештатным функционированием подсистем средств защиты информации.

5.3.10 Плановые проверки проводятся не реже одного раза в год в соответствии с Планом внутренних проверок контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее - План внутреннего контроля).

6. Порядок проведения внутренних проверок

6.1. В целях осуществления внутреннего контроля соответствия обработки

персональных данных установленным требованиям ответственный за обеспечение безопасности обработки персональных данных организует проведение периодических проверок условий обработки персональных данных.

6.2. Проверки соответствия обработки персональных данных установленным требованиям проводятся на основании утвержденного ответственным за обеспечение безопасности персональных данных плана внутренних проверок контроля соответствия обработки персональных данных требованиям к защите персональных данных, согласно приложению 1 к настоящим Правилам, или на основании поступившего в комитет письменного заявления о нарушениях правил обработки персональных данных (внеплановые проверки). Проведение внеплановой проверки организуется в течение 3-х рабочих дней с момента поступления соответствующего заявления.

6.3. Проверки осуществляются лицом, ответственным за обеспечение безопасности персональных данных либо комиссией, образуемой приказом председателя комитета.

6.4. В проведении проверки не может участвовать работник комитета или сотрудник сторонней организации, осуществляющей сопровождение информационной системы по государственному договору или договору подряда, прямо или косвенно заинтересованный в её результатах.

6.5. Количество плановых проверок зависит от:

- результатов проведения предыдущих проверок;

- критичности объекта (структурного подразделения, осуществляющего обработку и (или) защиту персональных данных, или процесса обработки персональных данных), по которому планируется проведение проверки;

- предложений руководства и специалистов структурных подразделений комитета.

6.6. Внеплановые внутренние проверки могут проводиться в следующих случаях:

- по результатам расследования выявленных нарушений требований законодательства в сфере персональных данных;

- по результатам внешних контрольных мероприятий, проводимых уполномоченным органом по защите прав субъектов персональных данных;

- при существенных изменениях процессов или процедур обработки и защиты персональных данных;

- при выявлении большого числа нарушений требований законодательства в сфере персональных данных или повторяемости одних и тех же нарушений от проверки к проверке;

- по указанию председателя комитета.

6.7. Проверки проводятся непосредственно на месте обработки персональных данных путем опроса либо, при необходимости, путем осмотра рабочих мест работников, участвующих в процессе обработки персональных данных.

6.8. По результатам проверки составляется протокол проведения внутренней проверки (приложение 2), результаты проверок фиксируются в журнале (приложение 5). Протокол подписывается ответственным за обеспечение безопасности персональных данных или членами комиссии.

6.9. При выявлении нарушений в сфере защиты персональных данных составляется акт (приложение 3), выявленные нарушения фиксируются в журнале (приложение 4).

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

6.11. Протоколы и акты хранятся у лица, ответственного за обеспечение безопасности персональных данных. Уничтожение протоколов и актов проводится лицом ответственным за обеспечение безопасности персональных данных самостоятельно в январе года следующего за проверочным годом. При необходимости протоколы могут храниться до полного устранения нарушений.

6.12. Результаты проведения внутренних проверок фиксируются в Отчете по результатам проведения внутренних проверок соответствия обработки персональных данных требованиям к защите персональных данных (далее по тексту - Отчет).

6.13. В Отчете должны быть указаны как минимум:

- основание проверки;
- вид проверки (плановая/внеплановая);
- цель проведения проверки;
- выявленные нарушения.

6.14. Отчет подписывается ответственным за обеспечение безопасности персональных данных либо комиссией, образованной приказом председателя комитета.

6.15. По результатам проведения внутреннего контроля ответственным за обеспечение безопасности персональных данных проводится анализ выявленных нарушений и разрабатывается план действий по устранению выявленных нарушений.

6.16. Результаты проведения внутреннего контроля и план действий по устранению выявленных нарушений доводятся до сведения председателя комитета для принятия решений о необходимости проведения работ по устранению выявленных нарушений.

Приложение 1
к Правилам осуществления внутреннего
контроля соответствия обработки
персональных данных требованиям
к защите персональных данных

ПЛАН
внутренних проверок контроля соответствия обработки персональных данных требованиям к защите персональных данных

Мероприятие	Периодичность	Исполнитель
Контроль соблюдения правил доступа к персональным данным	Еженедельно	Ответственный за обеспечение безопасности персональных данных
Контроль соблюдения режима защиты	Ежедневно	Ответственный за обеспечение безопасности персональных данных
Контроль выполнения антивирусной политики	Еженедельно	Ответственный за обеспечение безопасности персональных данных
Контроль выполнения парольной политики	Еженедельно	Ответственный за обеспечение безопасности персональных данных
Контроль соблюдения режима защиты при подключении к сетям общего пользования и (или) международного обмена	Еженедельно	Ответственный за обеспечение безопасности персональных данных
Проведение внутренних проверок на предмет выявления изменений в режиме обработки и защиты персональных данных	Ежегодно	Ответственный за обеспечение безопасности персональных данных
Контроль обновления ПО и единообразия применяемого ПО на всех элементах ГИС	Еженедельно	Ответственный за обеспечение безопасности персональных данных
Контроль обеспечения резервного копирования	Ежемесячно	Ответственный за обеспечение безопасности персональных данных
Организация анализа и пересмотра имеющихся угроз безопасности персональных данных, а так же предсказание появления новых, еще неизвестных, угроз	Ежегодно	Ответственный за обеспечение безопасности персональных данных
Поддержание в актуальном состоянии нормативноорганизационных документов	Ежемесячно	Ответственный за обеспечение безопасности персональных данных
Контроль запрета на использование беспроводных соединений	Ежемесячно	Ответственный за обеспечение безопасности персональных данных

Приложение 2
к Правилам осуществления внутреннего
контроля соответствия обработки
персональных данных требованиям
к защите персональных данных

ПРОТОКОЛ (ФОРМА) № _____
проведения внутренних проверок контроля соответствия обработки персональных данных требованиям к защите персональных данных в комитете региональной безопасности Курской области

Настоящий Протокол составлен в том, что «___» _____20__г.

_____
(комиссией) (должность, Ф.И.О. работника)
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:

Ответственный за обеспечение безопасности персональных данных

Приложение 3
к Правилам осуществления внутреннего
контроля соответствия обработки
персональных данных требованиям
к защите персональных данных

АКТ №

выявления нарушений в сфере защиты персональных данных

« _____» _____ 20__г.

Настоящий акт составлен в том, что в *(наименование структурного подразделения, где выявлено нарушение)* _____

(ФИО и должность лица, допустившего нарушение) допущено нарушение установленных требований в сфере защиты персональных данных и иной конфиденциальной информации.

Содержание нарушения _____

_____

Требования каких нормативных документов нарушены

_____

_____

Комиссия (или уполномоченное лицо), выявившая нарушения Подписи

(подпись) (Ф. И.О.)

(подпись) (Ф. И.О.)

(подпись) (Ф. И.О.)

С актом ознакомлены:

подпись лица, допустившего нарушение
_____ (ФИО) _____)

подпись руководителя структурного подразделения, где допущено нарушение
_____ (ФИО) _____

Приложение 4
к Правилам осуществления внутреннего
контроля соответствия обработки
персональных данных требованиям
к защите персональных данных

ЖУРНАЛ
регистрации выявленных нарушений в сфере защиты персональных данных

Начат «___» _____ 20__ г.

Окончен «___» _____ 20__ г.

№	Дата выявления нарушения	Подразделение, где выявлено нарушение и допустившее нарушение лицо (ФИО, должность)	Кем и при каких обстоятельствах выявлено нарушение (жалоба, плановая проверка и т.д.)	Содержание нарушения	Требования, каких нормативных документов нарушены	Корректирующие и предупреждающие действия по устранению нарушения и предотвращению нарушения в дальнейшем	Ответственное за устранение лицо выявленного нарушения лицо (ФИО, должность и его подпись)	Срок устранения нарушения	Отметка о контроле за выполнением (дата, ФИО и должность проверяющего)
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
1									
2									
3									

Приложение 5
к Правилам осуществления внутреннего
контроля соответствия обработки
персональных данных требованиям

ЖУРНАЛ
регистрации проверок в сфере защиты персональных данных

Начат «___» _____ 20__ г.

Окончен «___» _____ 20__ г.

№ п/п	Дата проверки	Вид проверки (плановая, внеплановая)	Основания проверки	Контрольные мероприятия	ФИО, должность проверяемого	Результат проверки	Номер, дата протокола результатов проверки	Результаты проверки	ФИО, должности членов комиссии	Подпись	
										Проверяемого	Членов комиссии
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
1											
2											

Приложение №5
к приказу комитета
региональной безопасности
Курской области
от 13.04.2021 № 47

Правила
работы с обезличенными данными
в случае обезличивания персональных данных

Настоящие Правила работы с обезличенными персональными данными разработаны с учетом Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных» и постановления Правительства РФ от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

Настоящие Правила определяют порядок работы с обезличенными персональными данными.

Настоящие Правила утверждаются председателем комитета.

Термины и определения

В соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»:

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

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.

Обезличивание персональных данных - действия, в результате которых:

невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

Условия обезличивания

Обезличивание персональных данных может быть проведено с целью ведения статистических данных, снижения ущерба от разглашения защищаемых персональных данных, снижения класса информационных систем персональных данных и по достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

Способы обезличивания при условии дальнейшей обработки персональных данных:

уменьшение перечня обрабатываемых сведений;

замена части сведений идентификаторами;

обобщение - понижение точности некоторых сведений;

понижение точности некоторых сведений (например, «Место жительства» может состоять из страны, индекса, города, улицы, дома и квартиры, а может быть указан только город);

деление сведений на части и обработка в разных информационных системах;

другие способы.

Способом обезличивания в случае достижения целей обработки или в случае

утраты необходимости в достижении этих целей является сокращение перечня персональных данных.

Для обезличивания персональных данных применяются способы явно не запрещенные законодательно.

Председатель комитета принимает решение о необходимости обезличивания персональных данных.

Начальники отделов, непосредственно осуществляющие обработку персональных данных, готовят предложения по обезличиванию персональных данных, обоснование такой необходимости и способ обезличивания.

Сотрудники подразделений, обслуживающих базы данных с персональными данными, совместно с ответственным за организацию обработки персональных данных, осуществляют непосредственное обезличивание выбранным способом.

Порядок работы с обезличенными персональными данными

Обезличенные персональные данные не подлежат разглашению и нарушению конфиденциальности.

Обезличенные персональные данные могут обрабатываться с использования и без использования средств автоматизации.

При обработке обезличенных персональных данных с использованием средств автоматизации необходимо соблюдение:

парольной политики;

антивирусной политики;

правил работы со съемными носителями (если они используется);

правил резервного копирования;

правил доступа в помещения, где расположены элементы информационных систем.

При обработке обезличенных персональных данных без использования средств автоматизации необходимо соблюдение:

правил хранения бумажных носителей;

правил доступа к ним и в помещения, где они хранятся.

Перечень
должностей служащих комитета региональной безопасности Курской области, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных, в случае обезличивания персональных данных

1. Председатель комитета.

2. Первый заместитель председателя комитета.

3. Начальник отдела безопасности информационных систем, организации закупок, делопроизводства.

4. Начальник отдела правового, кадрового обеспечения.

5. Начальник отдела финансового обеспечения, планирования, контроля.

6. Ведущий эксперт отдела безопасности информационных систем, организации закупок, делопроизводства.

Лист ознакомления

№ п/п	Ф.И.О.	Роспись
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		
11.		
12.		
13.		
14.		
15.		
16.		
17.		
18.		
19.		
20.		
21.		
22.		
23.		
24.		
25.		
26.		
27.		
28.		