

ОРГАНИЗАЦИЯ РАБОТЫ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ

Нормативно - правовые акты РФ в области организации обработки персональных данных

1. Федеральный Закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных», с изменениями внесенными Федеральным законом от 25 июля 2011 г. № 261-ФЗ»;

2. Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологий и о защите информации»;

3. Указ Президента Российской Федерации от 06 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера»;

4. Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

5. Постановление 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»;

6. Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении положения об особенностях обработки персональных данных осуществляемой без использования средств автоматизации»

7. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

Дополнительно:

8. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К), утверждены Решением Коллегии Гостехкомиссии России № 7.2 от 02.03.2001 г.

9. Информационное сообщение по вопросам защиты информации и обеспечения безопасности персональных данных при их обработке в информационных системах в связи с изданием приказа ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и приказа ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» № 240/22/2637 от 15 июля 2013 года.

№ п/п	Выполняемые мероприятия	пункт (статья) нормативного акта РФ
Основные организационные документы		
1	Уведомление в «Роскомнадзор» о намерении осуществлять обработку персональных данных	ст. 22 ч. 1 Федерального закона 152-ФЗ., ст. 1 пункт ж ПП № 211
2	Положение о порядке организации и проведения работ по защите информации (персональных данных)	п. 3.5 СТР-К

№ п/п	Выполняемые мероприятия	пункт (статья) нормативного акта РФ
3	Перечень сведений конфиденциального характера, подлежащих защите, утвержденный руководителем организации (Доведение его под роспись до всех должностных лиц в части касающейся)	п. 3.10, 5.1.3 СТР-К
4	Перечень лиц, доступ которых к ПД необходим для выполнения ими служебных (трудовых) обязанностей (<i>Ссылка на п. 17</i>)	ст. 13 п. в ПП 2012 г. № 1119
5	<p>Документы, утвержденные руководителем:</p> <ul style="list-style-type: none"> • !! Правила обработки персональных данных (политика оператора в отношении обработки ПД (в ред. 152-ФЗ)). <ul style="list-style-type: none"> - процедуры по выявлению и предотвращению нарушений законодательства РФ в сфере ПД (устранение последствий таких нарушений (в ред. 152-ФЗ)); - содержание обрабатываемых персональных данных для каждой цели - категории субъектов ПД; - сроки обработки, хранения и уничтожения ПД. • Правила рассмотрения запросов субъектов ПД. • Правила осуществления внутреннего контроля соответствия обработки ПД требованиям к их защите. • Правила работы с обезличенными данными. • Перечень должностей работников, ответственных за проведение мероприятий по обезличиванию ПД • Должностные обязанности (инструкция, регламент) ответственного за организацию обработки ПД • Типовое обязательство работника, осуществляющего обработку ПД (о прекращении им обработки ПД, в случае расторжения с ним контракта (трудового договора)). • Типовая форма согласия субъекта ПД на обработку ПД и форма разъяснения последствий отказа предоставления им своих ПД. • Порядок доступа работников в помещения, в которых ведется обработка ПД 	ст. 1 пункт б ПП 2012 года № 211 ст. 18.1 ч. 1 Федерального закона 152-ФЗ.,
6	Инструкция (перечень мер) по организации хранения носителей персональных данных, а также перечень лиц, ответственных за реализацию указанных мер (<i>ссылка на п. 18</i>). <i>Инструкция по организации учета, хранения, уничтожения, либо обезличивания персональных данных</i>	ст. 15 ПП 2008 г. № 687 ст. 7 Федерального закона 152-ФЗ.
7	Согласие (в письменной форме) субъекта ПД на обработку его ПД	ст. 9 ч. 4 Федерального закона 152-ФЗ.
8	Положение (Регламент, инструкция) об организации пропуска субъектов ПД на территорию оператора (<i>При необходимости</i>)	ст. 8 ПП 2008 г. № 687
Организационные документы по защите информации		
9	Оценка эффективности принимаемых мер по обеспечению безопасности ПД (<i>до ввода в эксплуатацию ИСПДн</i>) (форма и содержание документов определяются оператором самостоятельно) Не реже 1 раза в 3 года	ст. 19 ч. 2 Федерального закона 152-ФЗ.,
10	Модель угроз безопасности информации	п. 7 ПП 2012 г. № 1119
11	Перечень информационных систем персональных данных организации, утвержденный руководителем	ст. 1 пункт б ПП № 211
12	Правила доступа к ПД, обрабатываемых в ИСПДн.	ст. 19 ч. 2 Федерального закона 152-ФЗ.
Организационные мероприятия		
13	Организация внутреннего контроля соответствия обработки ПД установленным требованиям. Отчетный материал.	Ст. 1 пункт д ПП № 211,

№ п/п	Выполняемые мероприятия	пункт (статья) нормативного акта РФ
	Контроль за принимаемыми мерами по обеспечению безопасности ПД и уровня защищенности ИСПДн.	ст. 19 ч. 2 Федерального закона 152-ФЗ
14	Доведение под роспись до всех категорий должностных лиц требований законодательства РФ в области ПД, а также требований внутренних нормативных актов	ст. 1 пункт е ПП № 211 ст. 18.1 ч. 1 Федерального закона 152-ФЗ.,
Приказы		
15	Приказ о назначении ответственного за организацию обработки персональных данных в организации	ст. 18.1 ч. 1 Федерального закона 152-ФЗ.,
16	Приказ о назначении ответственного за обеспечение безопасности ПД в ИС <i>(от 3-го уровня защищенности ПД)</i>	ст. 14 ПП 2012 г. № 1119
17	Приказ о допуске (назначении) сотрудников к обработке персональных данных, без использования средств автоматизации <i>(ссылка на п.4)</i> (Доведение до назначенных сотрудников информации о категориях обрабатываемых ПД, особенностях и правилах осуществления такой обработки <i>(положения в соответствии с п.21)</i>), требований ПП 2008 г. № 687)	ст. 6 ПП 2008 г. № 687
18	Приказ об организации мест хранения материальных носителей персональных данных и ответственных за их сохранность <i>(Ссылка на п. 6)</i>	ст. 15 ПП 2008 г. № 687
Журналы и формы учетной документации		
19	Типовые формы документов, заполняемых субъектом ПД, оформленные в соответствии с п. 7 ПП 2008 г. № 687	п. 7 ПП 2008 г. № 687
20	Журнал учета машинных носителей информации	ст. 19 ч. 2 Федерального закона 152-ФЗ
21	Журнал (реестр, книга) учета, необходимый для пропуска субъекта ПД на территорию оператора <i>(при необходимости, в случае выполнения п. 8)</i>	п. 8 ПП 2008 г. № 687
ДРУГИЕ ОРГАНИЗАЦИОННЫЕ ДОКУМЕНТЫ		
22	Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации <i>(Дополнительно)</i>	ст. 3 ПП 2008 г. № 687
23	Приказ о назначении комиссии по определению уровня защищенности персональных данных	ПП 2012 г. № 1119
24	Акт установки уровня защищенности персональных данных при их обработке в ИСПДн	ПП 2012 г. № 1119
25	Приказ о назначении комиссии по уничтожению носителей ПД Приказ о назначении комиссии по уничтожению ПД Приказ о назначении комиссии по обезличиванию ПД	ст. 7 Федерального закона 152-ФЗ.
26	Формы актов на уничтожение ПД, носителей ПД, обезличивания ПД	ст. 7 Федерального закона 152-ФЗ.
ДОПОЛНИТЕЛЬНО		
27	План мероприятий по обеспечению безопасности ПДн	
28	Приложения к положению о порядке организации и проведения работ по защите информации (персональных данных) <i>(Ссылка на п. 2)</i> <ul style="list-style-type: none"> • Правила (инструкция) по парольной защите; • Правила (инструкция) по антивирусной защите; • Порядок работы с электронным журналом обращений пользователей информационной системы к ПД; • Порядок проведения служебного расследования нарушений режима информационной безопасности ИСПДн; 	

№ п/п	Выполняемые мероприятия	пункт (статья) нормативного акта РФ
	<ul style="list-style-type: none"> • Порядок приостановки предоставления ПДн в случае обнаружения нарушений порядка их обработки; • Инструкция о порядке резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации; 	
29	Журналы: <ul style="list-style-type: none"> • Журнал инструктажа сотрудников по вопросам ИБ; • Журнал учета обращений и запросов субъектов ПДн 	

* Перечень разрабатываемых документов может быть изменен по желанию оператора персональных данных.