СОВЕТ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОГО СОБРАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

КОМИТЕТ СОВЕТА ФЕДЕРАЦИИ ПО НАУКЕ, ОБРАЗОВАНИЮ, КУЛЬТУРЕ И ИНФОРМАЦИОННОЙ ПОЛИТИКЕ

ВРЕМЕННАЯ КОМИССИЯ СОВЕТА ФЕДЕРАЦИИ ПО РАЗВИТИЮ ИНФОРМАЦИОННОГО ОБЩЕСТВА

Материалы парламентских слушаний на тему «Законодательное обеспечение прав субъектов персональных данных при их автоматизированной обработке»

24 октября 2013 г.
Москва

Вносится членом Совета
Федерации Федерального
Собрания Российской Федерации
Р.У. Гаттаровым

ПРОЕКТ

ФЕДЕРАЛЬНЫЙ ЗАКОН

«О внесении изменений в Федеральный закон «О персональных данных»

Статья 1

Внести в Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных» (Собрание законодательства Российской Федерации, 2006, № 31, ст. 3451; 2009, № 48, ст. 5716; 2009, № 52 (1 ч.), ст. 6439; 2010, № 27, ст. 3407; 2010, № 31, ст. 4173; 2010, № 31, ст. 4196; 2010, № 49, ст. 6409; 2011, № 23, ст. 3263; 2011, № 31, ст. 4701; 2013, № 14, ст. 1651; 2013, № 30 (Часть I), ст. 4038) следующие изменения:

1) в статье 3:

дополнить пунктом 12 следующего содержания:

«12) субоператор персональных данных − лицо, осуществляющее обработку персональных данных по поручению оператора персональных данных;»;

2) статью 5 дополнить частью 8 следующего содержания:

Дополнить ст. 5 частью восьмой следующего содержания:

«8. Обработка персональных данных в составе сведений конфиденциального характера, связанных с профессиональной деятельностью, доступ к которым ограничен федеральным законом, осуществляется в порядке, установленном федеральным законом и принятыми в его исполнение нормативными правовыми актами для соответствующей информации. Обработка персональных данных в составе сведений конфиденциального характера, связанных с профессиональной деятельностью, доступ к которым ограничен федеральным законом, осуществляется в порядке, установленном настоящим Федеральным законом, если федеральный закон и принятые в его исполнение нормативные правовые акты не регулирует обработку соответствующей информации.»;

3) в статье 6:

в части 1 пункт 4 изложить в следующей редакции:

«4) обработка персональных данных необходима для предоставления субъекту персональных данных государственной или муниципальной услуги в соответствии с Федеральным законом от 27 июля 2010 года № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг»;»;

часть 3 изложить в следующей редакции:

«3. Оператор вправе поручить обработку персональных данных субоператору, если иное не предусмотрено федеральным законом, на основании заключаемого с субоператором договора, в том числе государственного или муниципального контракта, либо путем принятия государственным или муниципальным органом соответствующего акта (далее − поручение оператора). Субоператор обязан соблюдать принципы и правила обработки персональных данных, предусмотренные настоящим Федеральным законом. Субоператор вправе осуществлять обработку персональных данных, полученных от оператора, только в целях и на условиях, указанных в поручении оператора.»;

часть 4 изложить в следующей редакции:

«4. Субоператор не обязан получать согласие субъекта персональных данных на обработку его персональных данных.»;

часть 5 изложить в следующей редакции:

«5. Ответственность перед субъектом персональных данных за действия субоператора несет оператор. Субоператор несет ответственность перед оператором.»;

4) в статье 7:

абзац первый считать частью 1;

дополнить частью 2 следующего содержания:

«2. Обеспечение конфиденциальности персональных данных не требуется:

1) в отношении персональных данных, сделанных общедоступными субъектом персональных данных, а также в отношении обезличенных персональных данных;

2) в отношении персональных данных, которые подлежат опубликованию или обязательному раскрытию в соответствии с федеральным законом.»;

5) в статье 9:

в части 1 после слов «подтвердить факт его получения форме,» дополнить словами «в том числе дистанционно, путем использования электронных средств,

которые позволяют оператору удостовериться в согласии лица на обработку его персональных данных,»;

в части 4 слова «согласие в письменной форме субъекта персональных данных на обработку его персональных данных должно включать в себя, в частности:» заменить словами «В случаях, когда требуется согласие в письменной форме субъекта персональных данных на обработку его персональных данных, оно должно включать в себя, в частности:»;

6) часть 1 статьи 11 изложить в следующей редакции:

«Биологические и поведенческие характеристики субъекта персональных данных, на основании которых можно установить его личность и которые используются для автоматической идентификации при установлении личности субъекта персональных данных (биометрические персональные данные), могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных, за исключением случаев, предусмотренных частью 2 настоящей статьи.»;

7) в статье 12:

часть 4 дополнить пунктом 6 следующего содержания:

«6) обеспечения условиями договора, заключённого между лицами, осуществляющими обработку персональных данных, адекватной защиты прав субъектов персональных данных.»;

дополнить частью 5 следующего содержания:

«5. В случаях, когда собранные за пределами территории Российской Федерации персональные данные иностранного гражданина передаются на территорию Российской Федерации, положения настоящего Федерального закона не применяются к основаниям сбора и обработки этих персональных данных за пределами территории Российской Федерации, к основаниям и условиям их передачи оператору, находящемуся на территории Российской Федерации, а также к получению согласия и направлению уведомления об обработке таких персональных данных. К основаниям сбора и обработки персональных данных иностранного гражданина, собранных за пределами территории Российской Федерации, к основаниям и условиям их передачи оператору, находящемуся на территории Российской Федерации, а также к получению согласия и направлению уведомления об обработке таких персональных данных применяется законодательство иностранного государства, на территории которого были собраны персональные данные иностранного гражданина.»;

8) в статье 13:

в части 2:

слова «способов обозначения» заменить словом «обозначений»;

дополнить словами «которые являются персональными данными»;

в части 3 слова «способов обозначения» заменить словом «обозначений»;

9) в статье 18:

пункт 3 части 4 дополнить словами «либо подлежат опубликованию или обязательному раскрытию в соответствии с федеральным законом;»;

в пункте 4 части 4 после слов «для осуществления» дополнить словами «деятельности зарегистрированного средства массовой информации,»;

10) в статье 18.1:

в части 1 слова «если иное не предусмотрено настоящим Федеральным законом или другими федеральными законами.» исключить;

в пункте 3 части 1 слова «в соответствии со статьей 19 настоящего Федерального закона» исключить;

в части 3 слова «являющимися государственными или муниципальными органами» заменить словами «обрабатывающими персональные данные для целей предоставления государственных и муниципальных услуг или исполнения иных государственных и муниципальных функций.»;

11) статью 19 изложить в следующей редакции:

«1. Оператор и субоператор обязаны принимать или обеспечивать принятие правовых, организационных и технических мер для защиты персональных данных, обрабатываемых в информационных системах оператора, от неправомерного доступа, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных. Меры по обеспечению безопасности персональных данных при их обработке принимаются с учетом возможного вреда субъекту персональных данных, категории обрабатываемых персональных данных, условий и способов обработки персональных данных, актуальности угроз безопасности персональных данных.

2. Меры по обеспечению безопасности персональных данных при их обработке включают в себя, в частности:

1) определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

2) применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных;

3) оценку эффективности принимаемых мер по обеспечению безопасности персональных данных, в том числе до ввода в эксплуатацию информационной системы персональных данных;

4) обнаружение фактов несанкционированного доступа к персональным данным и принятие мер;

5) восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

6) установление правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учёта действий, совершаемых с персональными данными в информационной системе персональных данных;

7) контроль реализации мер по обеспечению безопасности персональных данных при их обработке;

8) создание системы защиты персональных данных при их обработке в информационной системе персональных данных;

9) назначение ответственного лица за обеспечение безопасности персональных данных при их обработке.

3. Правительство Российской Федерации с учетом частей 1 и 2 настоящей статьи устанавливает:

1) уровни защищенности персональных данных при их обработке операторами для целей предоставления государственных и муниципальных услуг или исполнения иных государственных и муниципальных функций в зависимости от угроз безопасности этих данных;

2) требования по обеспечению безопасности персональных данных при их обработке операторами для целей предоставления государственных и муниципальных услуг или исполнения иных государственных и муниципальных функций с учетом содержания обрабатываемых персональных данных, характера и способов их обработки;

3) требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных.

4. Состав и содержание установленных Правительством Российской Федерации требований по обеспечению безопасности персональных данных при

их обработке операторами для целей предоставления государственных и муниципальных услуг или исполнения иных государственных и муниципальных функций устанавливаются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий.

5. Меры по обеспечению безопасности персональных данных, обрабатываемых в составе сведений конфиденциального характера, связанных с профессиональной деятельностью, доступ к которым ограничен федеральным законом, осуществляется в порядке, установленном федеральным законом и принятыми в его исполнение нормативными правовыми актами для соответствующей информации. Меры по обеспечению безопасности персональных данных, обрабатываемых в составе сведений конфиденциального характера, связанных с профессиональной деятельностью, доступ к которым ограничен федеральным законом, осуществляется в порядке, установленном настоящим Федеральным законом, если федеральный закон и принятые в его исполнение нормативные правовые акты не устанавливают порядок обеспечения безопасности для соответствующей информации.

6. Контроль и надзор за выполнением операторами, обрабатывающими персональные данные для целей предоставления государственных и муниципальных услуг или исполнения иных государственных и муниципальных функций, установленных в соответствии с настоящим Федеральным законом требований по обеспечению безопасности персональных данных при их обработке для целей предоставления государственных и муниципальных услуг или исполнения иных государственных и муниципальных функций, осуществляется федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий и без права ознакомления с персональными данными, обрабатываемыми в информационных системах персональных данных.

7. Операторы или объединения операторов, за исключением операторов, обрабатывающих персональные данные для целей предоставления государственных и муниципальных услуг или исполнения иных государственных и муниципальных функций, вправе применять национальный или

международный стандарт обеспечения безопасности персональных данных при их обработке, либо разработать и утвердить собственный стандарт. Стандарты обеспечения безопасности персональных данных устанавливают меры по обеспечению безопасности персональных данных при их обработке в соответствии с частями 1 и 2 настоящей статьи.»;

12) в статье 22:

пункт 2 части 2 изложить в следующей редакции:

«2) полученных оператором в связи намерением субъекта персональных данных заключить договор или с заключением договора, стороной которого или выгодоприобретателем является субъект персональных данных, если персональные данные не распространяются, а также не предоставляются третьим лицам без согласия субъекта персональных данных или иных оснований, установленных законодательством Российской Федерации и используются оператором исключительно для оценки возможности заключения указанного договора, исполнения указанного договора и (или) заключения новых договоров с субъектом персональных данных;»;

в пункте 4 части 2 после слов «персональных данных» дополнить словами «или с согласия субъекта персональных данных»;

часть 4 изложить в следующей редакции:

«4. Уполномоченный орган по защите прав субъектов персональных данных в течение тридцати дней с даты поступления уведомления об обработке персональных данных вносит сведения, указанные в части 3 настоящей статьи, а также сведения о дате направления указанного уведомления в реестр операторов. Сведения, содержащиеся в реестре операторов, за исключением сведений действительных наименованиях, подчиненности и месте дислокации воинских частей, о средствах обеспечения безопасности персональных данных при их обработке и персональных данных лица ответственного за организацию обработки персональных данных, являются общедоступными.».

Президент
Российской Федерации

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

к проекту федерального закона «О внесении изменений в Федеральный закон «О персональных данных»

Законопроект разработан с целью совершенствования правового регулирования отношений в области обработки и защиты персональных данных путём устранения правовых коллизий, пробелов и внедрения новых подходов, которые отвечают мировым практикам и требованиям времени. Анализ практики применения Федерального закона от 27 июля 2006 г. № 152-ФЗ "О персональных данных" (далее – ФЗ-152) и международных нормативных правовых актов в обозначенной сфере, позволяет выделить ряд проблем, на решение которых направлен законопроект.

1. В правоприменительной практике возникла неопределённость относительно понимания категории биометрических персональных данных. Биометрические персональные данные являются таковыми только при соблюдении трёх условий одновременно: эти сведения должны характеризовать физиологические особенности человека; эти сведения должны позволять установить личность физического лица; эти сведения должны использоваться оператором для установления личности лица. Однако грамматическая конструкция ч. 1 ст. 11 ФЗ-152 позволяет понимать под биометрическими данными и те данные, которые не используются операторами для установления личности физического лица и использование которых не позволяет установить личность. Так, например, к обработке биометрических персональных данных можно отнести идентификацию работника по фотографии на пропуске или по фотографии работника на внутреннем корпоративном портале в справочнике сотрудников, также можно признать ксерокопии паспорта биометрическими персональными данными. Таким образом, практика показывает неоднозначное толкование норм ФЗ-152 в этой части.

Вопросы биометрической идентификации проработаны в ГОСТ Р ИСО/МЭК 19794-1-2008 «Автоматическая идентификация. Идентификация

биометрическая. Форматы обмена биометрическими данными». Соответственно, для устранения обозначенной неопределённости необходимо ввести изменения, определив биометрические персональные данные как биологические и поведенческие характеристики субъекта персональных данных, на основании которых можно установить его личность и которые используются для автоматической идентификации при установлении личности субъекта персональных данных.

2. Законодательством не установлен статус и требования к обработке идентификаторов сведений о физических лицах, используемых в государственных или муниципальных информационных системах персональных данных. Отсутствие правового статуса и требований к обработке идентификаторов персональных данных позволяет обрабатывать идентификаторы и связанные с ними сведения без соблюдения требований к обработке персональных данных, что приводит к нарушениям прав субъектов персональных данных и противоречит целям ФЗ-152. Особую остроту проблеме придает все более массовое использование алгоритмов автоматической обработки персональных данных.

Для решения обозначенной проблемы законопроектом предлагается внести изменения в ст. 13 ФЗ-152, указав, что различные обозначения принадлежности персональных данных, конкретного субъекта персональных данных, содержащиеся в соответствующей государственной или муниципальной информационной системе персональных данных, являются персональными данными.

3. В действующей редакции ФЗ-152 не решена проблема выбора норм законодательства о персональных данных или законодательства об иной информации по доступу при обработке персональных данных в составе иных сведений конфиденциального характера, связанных с профессиональной деятельностью.

Законопроектом вносятся изменения, согласно которым обработка персональных данных в составе сведений конфиденциального характера,

связанных с профессиональной деятельностью, доступ к которым ограничен федеральным законом, осуществляется в порядке, установленном специальным федеральным законом и принятыми в его исполнение нормативными правовыми актами для соответствующей информации. Однако обработка персональных данных в составе сведений конфиденциального характера, связанных с профессиональной деятельностью, доступ к которым ограничен федеральным законом, осуществляется в порядке, установленном ФЗ-152, если специальный федеральный закон и принятые в его исполнение нормативные правовые акты не регулирует обработку соответствующей информации. Данный подход основан на общепризнанном принципе разрешения конкуренции норм равной юридической силы, согласно которому должен действовать специальный закон (Lex specialis derogat generali).

4. Одним из условий обработки персональных данных является обеспечение их конфиденциальности. При этом в правоприменительной практике встречаются случаи требования обеспечения конфиденциальности персональных данных, которые являются общедоступными или обезличенными. Такое применение условия о конфиденциальности противоречит целям ФЗ-152, так как распространение общедоступных или обезличенных данных не может привести к нарушению права на неприкосновенность частной жизни, личную и семейную тайну.

В этой связи предлагается предусмотреть случаи исключения из условия о конфиденциальности обработки персональных данных. Так, согласно предлагаемой редакции, обеспечение конфиденциальности персональных данных не требуется:

а) в отношении персональных данных, сделанных общедоступными субъектом персональных данных, а также в отношении обезличенных персональных данных;

б) в отношении персональных данных, которые подлежат опубликованию или обязательному раскрытию в соответствии с федеральным законом.

Также законопроектом исключается необходимость уведомления об обработке персональных данных, которые подлежат обязательному раскрытию и опубликованию, поскольку у этих данных публичный статус.

5. В соответствии с ч. 3 ст. 6 ФЗ-152 оператор вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия государственным или муниципальным органом соответствующего акта (далее - поручение оператора).

Для передачи персональных данных другому лицу по поручению оператора необходимо получать согласие субъекта персональных данных на такую передачу. В условиях современного гражданского оборота это требование становится невыполнимым и ненужным. Необходимость получения согласия субъекта персональных данных на обработку его данных другим лицом по поручению оператора отсутствует постольку, поскольку ответственность перед субъектом персональных данных за действия другого лица, обрабатывающего данные по поручению оператора, несёт сам оператор, а также потому, что согласно принципам обработки персональных данных их обработка должна ограничиваться только заранее определёнными целями.

Для решения обозначенной проблемы законопроектом предлагается ввести понятие субоператора персональных данных. Субоператор персональных данных – это лицо, осуществляющее обработку персональных данных по поручению оператора персональных данных. На поручение обработки персональных данных субоператору согласие субъекта персональных данных не требуется. Соответственно, закрепляется, что субоператор вправе осуществлять обработку персональных данных, полученных от оператора, только в целях и на условиях, указанных в поручении оператора;

6. Ч. 1 ст. 9 ФЗ-152 предусматривает, что согласие на обработку персональных данных должно быть конкретным, информированным и сознательным, а также, что согласие на обработку персональных данных может

быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме. Развитие информационных технологий позволяет запрашивать согласие субъекта персональных данных на обработку персональных данных, соответствующее предъявляемым к согласию требованиям, дистанционно при помощи электронных средств. Практика осуществления контроля за соблюдением законодательства о персональных данных делает необходимым прямое указание в законе на то, что согласие на обработку персональных данных может быть получено дистанционно путем использования электронных средств, которые позволяют оператору удостовериться в согласии лица на обработку его персональных данных.

7. Одна из проблемных ситуаций заключается в том, что государственные и муниципальные органы осуществляют передачу персональных данных без согласия и уведомления субъектов персональных данных, мотивируя это тем, что тем самым они обеспечивают предоставление государственных или муниципальных услуг. В целях совершенствования ФЗ-152 в части, касающейся обработки персональных данных государственными и муниципальными органами, законопроектом предлагается следующее. Необходимо ограничить возможность органов власти обрабатывать персональные данные без согласия субъекта персональных данных только целями предоставления государственных или муниципальных услуг, в соответствии Федеральным законом от 27 июля 2010 года № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг».

8. Регулируя отношения по трансграничной передаче персональных данных, действующее законодательство не регулирует вопросы о выборе норм российского или соответствующего иностранного законодательства в ситуации, когда необходимо применять иностранное законодательство. Речь идет о случаях обработки персональных данных иностранного гражданина, собранных за пределами территории РФ.

Для устранения пробела в правовом регулировании законопроектом предлагается предусмотреть, что к основаниям сбора и обработки персональных данных иностранного гражданина, собранных за пределами территории РФ, к основаниям и условиям их передачи оператору, находящемуся на территории России, а также к получению согласия и направлению уведомления об обработке таких персональных данных применяется законодательство иностранного государства, на территории которого были собранны персональные данные иностранного гражданина.

Для целей совершенствования правового регулирования трансграничной передачи персональных данных законопроект расширяет перечень оснований для трансграничной передачи персональных данных, устанавливая возможность передачи персональных данных за границу, если условия договора обеспечивают адекватную защиту персональных данных или если оператор персональных данных принял внутренние правила, которые обеспечивают адекватную защиту.

9. Мировой опыт вообще и европейский в частности свидетельствуют о том, что требования по обеспечению безопасности персональных данных не должны быть едины для операторов, которые являются частными организациями или индивидуальными предпринимателями, и для операторов – органов власти. Принципиальное отличие частной и публичной групп операторов персональных данных заключается в следующем. Частные операторы собирают и обрабатывают персональные данные по воле физических лиц (работников частных организаций, получателей услуг частного характера, потребителей различной продукции и т.д.), и они (частные операторы) заинтересованы в охране персональных данных, так как их утечка сказывается на их привлекательности как работодателей или как производителей той или иной продукции. Публичные операторы данной заинтересованностью не обладают, и сбор персональных данных осуществляется не по воле субъекта, а в силу необходимости осуществления различных публичных функций. В отличие от частых операторов, публичным операторам на обеспечение безопасности персональных данных выделяются бюджетные средства.

Частные операторы персональных данных вынуждены выполнять требования по защите персональных данных ранее содержавшиеся в ведомственных нормативных актах ФСТЭК РФ и ФСБ РФ. Устаревшие методы и способы защиты государственной тайны обязательны для пяти с лишним миллионов операторов персональных данных.

С целью совершенствования правового регулирования мер по обеспечению безопасности персональных данных законопроектом предлагается концепция, основанная на дифференциации регулирования обеспечения безопасности персональных данных в публичных и частных информационных системах.

Защиту персональных данных в информационных системах операторов, обрабатывающих персональные данные для целей предоставления государственных и муниципальных услуг или исполнения иных государственных и муниципальных функций, необходимо осуществлять по требованиям Правительства РФ и профильных ведомств.

Для частных операторов персональных данных требования Правительства РФ и профильных ведомств в области обеспечения безопасности персональных данных должны носить рекомендательный характер. Частные операторы персональных данных вправе применять национальный или международный стандарт обеспечения безопасности персональных данных либо разработать и утвердить собственный стандарт.

10. Ч. 4 ст. 18 ФЗ-152 предусмотрены исключения из обязанности оператора персональных данных предоставлять субъекту персональных данных определённую информацию, связанную с обработкой персональных данных, полученных не от субъекта персональных данных. Одним из таких исключений является случай обработки персональных данных для статистических или иных исследовательских целей, для осуществления профессиональной деятельности журналиста либо научной, литературной или иной творческой деятельности. Вместе с тем на основании п. 8 ч. 1 ст. 6 ФЗ-152 разрешено обрабатывать персональные данные без согласия субъекта персональных данных для

осуществления профессиональной деятельности журналиста и (или) законной деятельности средства массовой информации либо научной, литературной или иной творческой деятельности.

Законопроектом предлагается распространить исключение из обязанности предоставлять субъекту персональных данных определённую информацию, связанную с обработкой персональных данных также для осуществления деятельности зарегистрированного средства массовой информации.

12. Законопроектом предлагается запретить публикацию в открытом доступе сведений о дислокации воинских частей, а также персональных данных лиц, ответственных за обработку персональных данных у оператора.

Принятие изменений, предусмотренных законопроектом, устранит обозначенные проблемы и усовершенствует правовое регулирование в области обработки и защиты персональных данных.

Проект поправок в Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных» (в ред. от 23.10.2013)

Существующая редакция закона	Редакция предлагаемого изменения	Комментарий
	Дополнить ст. 3 пунктами следующего содержания: ***2.2) субоператор персональных данных – лицо, осуществляющее обработку персональных данных по поручению оператора персональных данных;***	**П. 2.2. ст. 3** Введение понятия субоператора ПДн направлено на закрепление правового статуса лица, обрабатывающего персональные данные по поручению оператора. (Подробнее см.: изменения ст. 6).
Ст. 5. 1. Обработка персональных данных должна осуществляться на законной и справедливой основе. 2. Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных. 3. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой. 4. Обработке подлежат только персональные данные, которые отвечают целям их обработки. 5. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки. 6. При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных. 7. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого	**Дополнить ст. 5 частью восьмой следующего содержания:** ***8. Обработка персональных данных в составе сведений конфиденциального характера, связанных с профессиональной деятельностью, доступ к которым ограничен федеральным законом, осуществляется в порядке, установленном федеральным законом и принятыми в его исполнение нормативными правовыми актами для соответствующей информации. Обработка персональных данных в составе сведений конфиденциального характера, связанных с профессиональной деятельностью, доступ к которым ограничен федеральным законом, осуществляется в порядке, установленном настоящим Федеральным законом, если федеральный закон и принятые в его исполнение нормативные правовые акты не регулирует обработку соответствующей информации.***	ПДн во многих случаях являются составной частью других сведений конфиденциального характера, определенных Указом Президента РФ № 188 от 06.03.1997 года, порядок обработки и защиты которых установлен отраслевым законодательством, например, о банковской деятельности, о связи и т.п. В законодательстве РФ отсутствуют однозначные критерии для определения правового статуса сведений, которые являются ПДн и одновременно могут относиться к другим сведениям конфиденциального характера. Требования законов к обработке и обеспечению безопасности разных категорий сведений различны. Однако они, как правило, обрабатываются в одних и тех же информационных системах оператора (обладателя информации). Неоднозначность требований в разных законах и нормативных правовых актах является источником правоприменительных рисков для операторов по причине невозможности одновременного выполнения всех требований. Создаются правовые коллизии при определении приоритета применения законов и требований, которые должны быть выполнены. Например, статьи 53 и 63 Федерального закона № 126-ФЗ «О связи» регулирует порядок обработки «сведений об абоненте» и «тайны связи», которые

требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.		одновременно могут являться ПДн. Требования к обработке и обеспечению безопасности указанных сведений и ПДн различны. Учитывая наличие отраслевых особенностей процессов обработки ПДн, предлагается осуществлять организацию обработки и обеспечение безопасности ПДн, обрабатываемых в составе иной информации конфиденциального характера, связанной с профессиональной деятельностью, по требованиям отраслевого законодательства.
П.4 ч. 1 ст. 6 4) обработка персональных данных необходима для исполнения полномочий федеральных органов исполнительной власти, органов государственных внебюджетных фондов, исполнительных органов государственной власти субъектов Российской Федерации, органов местного самоуправления и функций организаций, участвующих в предоставлении соответственно государственных и муниципальных услуг, предусмотренных Федеральным законом от 27 июля 2010 года № 210-ФЗ "Об организации предоставления государственных и муниципальных услуг", включая регистрацию субъекта персональных данных на едином портале государственных и муниципальных услуг и (или) региональных порталах государственных и муниципальных услуг;	**П. 4 ч. 1 ст. 6** 4) ***обработка персональных данных необходима для предоставления субъекту персональных данных государственной или муниципальной услуги в соответствии с Федеральным законом от 27 июля 2010 года № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг».*** **Ч. 3 ст. 6** ***3. Оператор вправе поручить обработку персональных данных субоператору, если иное не предусмотрено федеральным законом, на основании заключаемого с субоператором договора, в том числе государственного или муниципального контракта, либо путем принятия государственным или муниципальным органом соответствующего акта (далее – поручение оператора). Субоператор обязан соблюдать принципы и правила обработки персональных данных, предусмотренные настоящим Федеральным законом. Субоператор вправе осуществлять обработку персональных данных, полученных от оператора, только в целях и на условиях, указанных в поручении оператора.*** **Ч. 4-5 ст. 6** ***4. Субоператор не обязан получать согласие субъекта***	**П. 4 ч. 1 ст. 6** Предлагаемое изменение направлено на конкретизацию исключения из общего правила об обработке ПДн только с согласия субъекта ПДн, согласно которому ПДн могут обрабатываться без согласия субъекта ПДн, если это необходимо «для обеспечения предоставления» государственной или муниципальной услуги. Необходимость конкретизации данного исключения возникла вследствие того, что оно фактически позволяет обрабатывать ПДн без согласия субъекта ПДн всему государственному аппарату, так как в конечном итоге одной из основных целей его деятельности является предоставление государственных и муниципальных услуг. **Ч. 3-5 ст. 6** П. 5 ч. 1 ст. 6 ФЗ-152 разрешает оператору ПДн обрабатывать ПДн в целях исполнения договора с субъектом ПДн без получения согласия субъекта ПДн. Однако ч. 3 ст. 6 ФЗ-152 предусмотрено, что оператор вправе поручить обработку ПДн другому лицу с согласия субъекта, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора.

	персональных данных на обработку его персональных данных. ***5. Ответственность перед субъектом персональных данных за действия субоператора несет оператор. Субоператор несет ответственность перед оператором.***	На практике операторам ПДн требуется получать отдельные согласия субъектов ПДн на передачу ПДн третьим лицам даже в случаях, когда привлечение таких лиц осуществляется для целей исполнения договора, заключенного между субъектом ПДн и оператором ПДн. При этом необходимо указывать конкретных лиц, которые участвуют в обработке ПДн по поручению оператора ПДн. Положения ГК РФ не содержат каких-либо общих ограничений для привлечения третьих лиц к исполнению договора. Обязанность получать отдельные согласия субъектов ПДн в случаях привлечения подрядчиков, исполнителей отдельных обязательств по договору, заключенному оператором ПДн с субъектом ПДн, существенно и необоснованно затрудняет гражданский оборот. После заключения договора с субъектом ПДн может меняться состав лиц, привлекаемых для обработки ПДн в целях выполнения договора. Получение дополнительного согласия от субъектов ПДн на обработку ПДн этими лицами является в общем случае не выполнимой для оператора ПДн задачей.
Ст. 7 Операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.	**Дополнить ст. 7 частью второй следующего содержания:** ***2. Обеспечение конфиденциальности персональных данных не требуется:*** ***1) в отношении персональных данных, сделанных общедоступными субъектом персональных данных, а также в отношении обезличенных персональных данных;*** ***2) в отношении персональных данных, которые подлежат опубликованию или обязательному раскрытию в соответствии с федеральным законом;***	Данные изменения направлены на устранение логической противоречивости в обеспечении конфиденциальности ПДн. Действующее законодательство обязывает обеспечивать конфиденциальность любых ПДн, в том числе и общедоступных данных, а также в отношении данных, которые подлежат опубликованию или обязательному раскрытию в соответствии с федеральным законом. Необходимо понимать, что целью законодательства о ПДн является защита конституционных прав и свобод. Представляется, что если данные являются общедоступными или обезличенными, то их распространение не может нарушить конституционных прав. Следовательно,

		обеспечение конфиденциальности в отношении обозначенных данных является излишним для выполнения целей законодательства.
Ч. 1 ст. 9 1. Субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку персональных данных должно быть конкретным, информированным и сознательным. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом. В случае получения согласия на обработку персональных данных от представителя субъекта персональных данных полномочия данного представителя на дачу согласия от имени субъекта персональных данных проверяются оператором. **Ч. 4 ст. 9** 4. В случаях, предусмотренных федеральным законом, обработка персональных данных осуществляется только с согласия в письменной форме субъекта персональных данных. Равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью. Согласие в письменной форме субъекта персональных данных на обработку его персональных данных должно включать в себя, в частности:	**Ч. 1 ст. 9** 1. Субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку персональных данных должно быть конкретным, информированным и сознательным. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, ***в том числе дистанционно, путем использования электронных средств, которые позволяют оператору удостовериться в согласии лица на обработку его персональных данных,*** если иное не установлено федеральным законом. **Ч. 4 ст. 9** 4. В случаях, предусмотренных федеральным законом, обработка персональных данных осуществляется только с согласия в письменной форме субъекта персональных данных. Равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью. ***В случаях, когда требуется согласие в письменной форме субъекта персональных данных на обработку его персональных данных, оно должно включать в себя***, в частности:	**Ч. 1 ст. 9** Развитие электронных коммуникаций обуславливает необходимость законодательного закрепления возможности дистанционного способа получения согласия на обработку ПДн. Так предлагается ввести положение о том, что согласие может быть получено дистанционно, путем использования электронных средств, которые позволяют оператору удостовериться в согласии лица на обработку его ПДн. **Ч. 4 ст. 9** В практике обработки персональных данных возникает неопределенность в вопросе о том, что должно содержать согласие субъекта ПДн в конкретном случае, когда такое согласие требуется. Проблема заключается в том, что есть установленные случаи, когда согласие субъекта ПДн должно быть выражено в письменной форме, при этом требования к содержанию письменной формы контролирующий орган требует применять и к тем согласиям, которые могут быть выражены и в иной форме. Предлагаемые изменения уточняют, что требования к содержанию согласия распространяются только на те случаи, когда такое согласие должно быть дано в письменной форме. В отношении согласия, выраженного не в письменной форме, есть общее требование, а именно такое согласие должно обеспечивать возможность подтверждения факта его получения.

Ч. 1 ст. 11 1. Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются оператором для установления личности субъекта персональных данных, могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных, за исключением случаев, предусмотренных частью 2 настоящей статьи.	**Ч. 1 ст. 11** 1. ***Биологические и поведенческие характеристики субъекта персональных данных, на основании которых можно установить его личность и которые используются для автоматической идентификации при установлении личности субъекта персональных данных*** (биометрические персональные данные), могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных, за исключением случаев, предусмотренных частью 2 настоящей статьи.	**Ч. 1 ст. 11** Определение в статье 11 Закона категории «биометрических ПДн» и порядка их обработки в целях идентификации субъекта ПДн неоднозначны. К обработке биометрических ПДн в целях идентификации можно отнести, например, идентификацию работника по фотографии на пропуске или размещение фотографии работника на внутреннем корпоративном портале в справочнике сотрудников, что не является предметом защиты биометрических ПДн при их автоматизированной обработке и создает ситуацию неоднозначного толкования норм ФЗ-152. Например, регулятор определяет наличие сканированной копии паспорта как обработку биометрических ПДн и требует брать согласие на это у субъекта ПДн. Однако операторы используют сканированные копии паспортов не для идентификации личности, которая может проводиться только при сличении фотографии с самим субъектом, а для контроля действий операторов и подтверждения проведения процедуры.

Ч. 4 ст. 12 4. Трансграничная передача персональных данных на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных, может осуществляться в случаях: 1) наличия согласия в письменной форме субъекта персональных данных на трансграничную передачу его персональных данных; 2) предусмотренных международными договорами Российской Федерации; 3) предусмотренных федеральными законами, если это необходимо в целях защиты основ конституционного строя Российской Федерации, обеспечения обороны страны и безопасности государства, а также обеспечения безопасности устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства; 4) исполнения договора, стороной которого является субъект персональных данных; 5) защиты жизни, здоровья, иных жизненно важных интересов субъекта персональных данных или других лиц при невозможности получения согласия в письменной форме субъекта персональных данных.	**Дополнить ч. 4 ст. 12 пунктом следующего содержания:** ***6) обеспечения условиями договора, заключённого между лицами, осуществляющими обработку персональных данных, адекватной защиты прав субъектов персональных данных.*** **Дополнить ст. 12 частью пятой следующего содержания:** ***В случаях, когда собранные за пределами территории Российской Федерации персональные данные иностранного гражданина передаются на территорию Российской Федерации, положения настоящего Федерального закона не применяются к основаниям сбора и обработки этих персональных данных за пределами территории Российской Федерации, к основаниям и условиям их передачи оператору, находящемуся на территории Российской Федерации, а также к получению согласия и направлению уведомления об обработке таких персональных данных. К основаниям сбора и обработки персональных данных иностранного гражданина, собранных за пределами территории Российской Федерации, к основаниям и условиям их передачи оператору, находящемуся на территории Российской Федерации, а также к получению согласия и направлению уведомления об обработке таких персональных данных применяется законодательство иностранного государства, на территории которого были собранны персональные данные иностранного гражданина.***	**П. 6-7 ч. 4 ст. 12** Сопоставление российского законодательства в сфере трансграничной передачи ПДн с международной практикой регулирования данной сферы, прежде всего европейским опытом такого регулирования, показывает отсутствие должных правовых мер, направленных на реализацию принципа свободного обмена информацией. В первую очередь, речь идет об отсутствии законодательных условий, позволяющих использовать при трансграничной передаче гибкие и эффективные правовые механизмы, позволяющие обеспечить адекватный уровень защиты ПД, такие как: 1) корпоративные правила, имеющие обязательную силу в отношении конкретного юридического лица или группы лиц; 2) индивидуальные договорные условия. **Ч. 5 ст. 12** В изменениях, которыми ст. 12 дополняется новой частью, речь идёт о коллизионной норме, которая определяет подлежащее применению право к отношениям, осложнённым иностранным элементом, то есть когда российским оператором обрабатываются ПДн иностранного гражданина. Суть предложения заключается в том, что ФЗ-152 не должен распространяться на отношения иностранного гражданина и иностранного оператора в части сбора и обработки ПДн за пределами территории России. К таким отношениям должно применяться иностранное законодательство.

Ст. 13 1. Государственные органы, муниципальные органы создают в пределах своих полномочий, установленных в соответствии с федеральными законами, государственные или муниципальные информационные системы персональных данных. 2. Федеральными законами могут быть установлены особенности учета персональных данных в государственных и муниципальных информационных системах персональных данных, в том числе использование различных способов обозначения принадлежности персональных данных, содержащихся в соответствующей государственной или муниципальной информационной системе персональных данных, конкретному субъекту персональных данных. 3. Права и свободы человека и гражданина не могут быть ограничены по мотивам, связанным с использованием различных способов обработки персональных данных или обозначения принадлежности персональных данных, содержащихся в государственных или муниципальных информационных системах персональных данных, конкретному субъекту персональных данных. Не допускается использование оскорбляющих чувства граждан или унижающих человеческое достоинство способов обозначения принадлежности персональных данных, содержащихся в государственных или муниципальных информационных системах персональных данных, конкретному субъекту персональных данных. 4. В целях обеспечения реализации прав субъектов персональных данных в связи с обработкой их персональных данных в государственных или муниципальных информационных системах персональных данных может быть создан государственный регистр населения, правовой статус которого и порядок работы с которым устанавливаются федеральным законом.	**Ч. 2 ст. 13 изложить в следующей редакции:** Федеральными законами могут быть установлены особенности учета персональных данных в государственных и муниципальных информационных системах персональных данных, в том числе использование различных ***обозначений*** принадлежности персональных данных, содержащихся в соответствующей государственной или муниципальной информационной системе персональных данных, конкретному субъекту персональных данных, ***которые являются персональными данными.*** **Ч.3 ст. 13 изложить в следующей редакции:** Права и свободы человека и гражданина не могут быть ограничены по мотивам, связанным с использованием различных способов обработки персональных данных или обозначения принадлежности персональных данных, содержащихся в государственных или муниципальных информационных системах персональных данных, конкретному субъекту персональных данных. Не допускается использование оскорбляющих чувства граждан или унижающих человеческое достоинство ***обозначений*** принадлежности персональных данных, содержащихся в государственных или муниципальных информационных системах персональных данных, конкретному субъекту персональных данных.	**Ч. 2, 3, 3.1 ст. 13** Данные изменения направлены на закрепление правового статуса идентификаторов ПДн. В данном случае на идентификаторы ПДн предлагается распространить некоторые принципы и правила обработки ПДн.

П. 3 ч. 4 ст. 18 3) персональные данные сделаны общедоступными субъектом персональных данных или получены из общедоступного источника; **П. 4 ч. 4 ст. 18** 4) оператор осуществляет обработку персональных данных для статистических или иных исследовательских целей, для осуществления профессиональной деятельности журналиста либо научной, литературной или иной творческой деятельности, если при этом не нарушаются права и законные интересы субъекта персональных данных;	**П. 3 ч. 4 ст. 18** 3) персональные данные сделаны общедоступными субъектом персональных данных, получены из общедоступного источника, ***либо подлежат опубликованию или обязательному раскрытию в соответствии с федеральным законом***; **П. 4 ч. 4 ст. 18** 4) оператор осуществляет обработку персональных данных для статистических или иных исследовательских целей, для осуществления ***деятельности зарегистрированного средства массовой информации***, профессиональной деятельности журналиста либо научной, литературной или иной творческой деятельности, если при этом не нарушаются права и законные интересы субъекта персональных данных;	**П. 3 ч. 4 ст. 18** Предлагается исключить необходимость уведомления об обработке ПДн, которые подлежат обязательному раскрытию и опубликованию, поскольку у них публичный статус. **П. 4 ч. 4 ст. 18** Необходимо прямо включить указание на деятельность самого средства массовой информации, а не только на профессиональную деятельность журналиста.
Ч. 1 ст. 18.1 1. Оператор обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных настоящим Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами. Оператор самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных настоящим Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено настоящим Федеральным законом или другими федеральными законами. **П. 3 ч. 1 ст. 18.1** 3) применение правовых, организационных и технических мер по обеспечению безопасности персональных данных в соответствии со статьей 19 настоящего Федерального закона;	**Ч. 1 ст. 18.1** 1. Оператор обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных настоящим Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами. Оператор самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных настоящим Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами, ~~***если иное не предусмотрено настоящим Федеральным законом или другими федеральными законами.***~~ **П. 3 ч. 1 ст. 18.1** 3) применение правовых, организационных и технических мер по обеспечению безопасности персональных данных ~~***в соответствии со статьей 19 настоящего Федерального закона***~~; **Ч. 3 ст. 18.1**	**Ч. 1, п. 3 ч. 1 ст. 18.1** Необходимо указать, что мероприятия по защите должен выбирать сам оператор ПДн, понимающий специфику обработки ПДн в своей отрасли. (Подробнее См.: изменения ст. 19.) Обязательные требования по обеспечению безопасности ПДн должны устанавливаться только для государственных и муниципальных информационных систем, для которых бюджет на выполнение мер защиты определяется государством. Для иных информационных систем меры защиты должны выбираться оператором на основе международных или национальных стандартов по защите ПДн. **Ч. 3 ст. 18.1** Ч. 3 ст. 18.1 ФЗ-152 направлена на установление более жестких требований к выполнению обязанностей, предусмотренных законом, в отношении государственных и муниципальных

Ч. 3 ст. 18.1 3. Правительство Российской Федерации устанавливает перечень мер, направленных на обеспечение выполнения обязанностей, предусмотренных настоящим Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами.	3.Правительство Российской Федерации устанавливает перечень мер, направленных на обеспечение выполнения обязанностей, предусмотренных настоящим Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами, операторами, ***обрабатывающими персональные данные для целей предоставления государственных и муниципальных услуг или исполнения иных государственных и муниципальных функций***.	органов. Данная мера представляется оправданной с учетом повышенных рисков при обработке ПДн данными субъектами. Между тем, повышенные риски при обработке ПДн имеют место не только при их обработке государственными и муниципальными органами, но и при их обработке иными субъектами в публичных целях (например, организациями, участвующими в предоставлении государственных и муниципальных услуг). В связи с этим предлагается распространить устанавливаемый Правительством РФ перечень мер по обеспечению выполнения обязанностей, установленных настоящим федеральным законом, на всех операторов, осуществляющих обработку ПДн в публичных целях.
Ст. 19 1. Оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных. 2. Обеспечение безопасности персональных данных достигается, в частности: 1) определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных; 2) применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;	**Ст. 19** ***1. Оператор и субоператор обязаны принимать или обеспечивать принятие правовых, организационных и технических мер для защиты персональных данных, обрабатываемых в информационных системах оператора, от неправомерного доступа, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных. Меры по обеспечению безопасности персональных данных при их обработке принимаются с учетом возможного вреда субъекту персональных данных, категории обрабатываемых персональных данных, условий и способов обработки персональных данных, актуальности угроз безопасности персональных данных.*** ***2. Меры по обеспечению безопасности персональных данных при их обработке включают в себя, в частности:*** ***1) определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных;*** ***2) применение организационных и технических мер по***	**Ст. 19** Изменения представляют собой новый концептуальный подход к мерам по обеспечению безопасности ПДн при их обработке. Его суть заключается в том, что должна быть разница между регулированием безопасности при обработке ПДн в государственных и муниципальных органах и регулированием данной безопасности в частных организациях. В целях учета отраслевых особенностей обработки ПДн и гармонизации мер по обеспечению безопасности ПДн с международными стандартами предлагается реализовать подход, учитывающий правовой статус информационных систем и дифференциацию мер защиты для государственных, муниципальных и иных информационных систем, что предусмотрено ст. 13 и 16 ФЗ № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Согласно предлагаемому подходу необходимо: 1. Дифференцировать регулирование вопросов обеспечения безопасности ПДн в

3) применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации; 4) оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных; 5) учетом машинных носителей персональных данных; 6) обнаружением фактов несанкционированного доступа к персональным данным и принятием мер; 7) восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним; 8) установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных; 9) контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных. 3. Правительство Российской Федерации с учетом возможного вреда субъекту персональных данных, объема и содержания обрабатываемых персональных данных, вида деятельности, при осуществлении которого обрабатываются персональные данные, актуальности угроз безопасности персональных данных устанавливает: 1) уровни защищенности персональных данных при их обработке в информационных системах персональных данных в зависимости от угроз безопасности этих данных; 2) требования к защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных; 3) требования к материальным носителям	***обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных;*** ***3) оценку эффективности принимаемых мер по обеспечению безопасности персональных данных, в том числе до ввода в эксплуатацию информационной системы персональных данных;*** ***4) обнаружение фактов несанкционированного доступа к персональным данным и принятие мер;*** ***5) восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;*** ***6) установление правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учёта действий, совершаемых с персональными данными в информационной системе персональных данных;*** ***7) контроль реализации мер по обеспечению безопасности персональных данных при их обработке;*** ***8) создание системы защиты персональных данных при их обработке в информационной системе персональных данных;*** ***9) назначение ответственного лица за обеспечение безопасности персональных данных при их обработке.*** ***3. Правительство Российской Федерации с учетом частей 1 и 2 настоящей статьи устанавливает:*** ***1) уровни защищенности персональных данных при их обработке операторами для целей предоставления государственных и муниципальных услуг или исполнения иных государственных и муниципальных функций в зависимости от угроз безопасности этих данных;*** ***2) требования по обеспечению безопасности персональных данных при их обработке операторами для целей предоставления государственных и муниципальных услуг или исполнения иных государственных и муниципальных функций с учетом содержания обрабатываемых персональных данных, характера и способов их обработки;***	государственных, муниципальных и иных информационных системах. Защиту ПДн в государственных и муниципальных информационных системах персональных данных (далее – ИС ПДн) осуществлять по требованиям Правительства РФ. Защиту ПДн в иных ИС ПДн осуществлять на основе рекомендаций международных или национальных стандартов по ИБ. 2. В целях учета отраслевых особенностей обработки ПДн, обрабатываемых в составе иных сведений конфиденциального характера, связанных с профессиональной деятельностью (состав сведений см. в пункте 4 Указа Президента РФ № 188), обеспечение их безопасности осуществлять по требованиям Федеральных законов, регламентирующих деятельность в соответствующей профессиональной области.

биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных. 4. Состав и содержание необходимых для выполнения установленных Правительством Российской Федерации в соответствии с частью 3 настоящей статьи требований к защите персональных данных для каждого из уровней защищенности, организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных устанавливаются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий. 5. Федеральные органы исполнительной власти, осуществляющие функции по выработке государственной политики и нормативно-правовому регулированию в установленной сфере деятельности, органы государственной власти субъектов Российской Федерации, Банк России, органы государственных внебюджетных фондов, иные государственные органы в пределах своих полномочий принимают нормативные правовые акты, в которых определяют угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, с учетом содержания персональных данных, характера и способов их обработки. 6. Наряду с угрозами безопасности персональных данных, определенных в нормативных правовых актах, принятых в соответствии с частью 5 настоящей статьи, ассоциации, союзы и иные объединения операторов своими решениями вправе определить дополнительные угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных,	***3) требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных.*** ***4. Состав и содержание установленных Правительством Российской Федерации требований по обеспечению безопасности персональных данных при их обработке операторами для целей предоставления государственных и муниципальных услуг или исполнения иных государственных и муниципальных функций устанавливаются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий.*** ***5. Меры по обеспечению безопасности персональных данных, обрабатываемых в составе сведений конфиденциального характера, связанных с профессиональной деятельностью, доступ к которым ограничен федеральным законом, осуществляется в порядке, установленном федеральным законом и принятыми в его исполнение нормативными правовыми актами для соответствующей информации. Меры по обеспечению безопасности персональных данных, обрабатываемых в составе сведений конфиденциального характера, связанных с профессиональной деятельностью, доступ к которым ограничен федеральным законом, осуществляется в порядке, установленном настоящим Федеральным законом, если федеральный закон и принятые в его исполнение нормативные правовые акты не устанавливают порядок обеспечения безопасности для соответствующей информации.*** ***6. Контроль и надзор за выполнением операторами, обрабатывающими персональные данные для целей предоставления государственных и муниципальных услуг или исполнения иных государственных и муниципальных функций, установленных в***	

эксплуатируемых при осуществлении определенных видов деятельности членами таких ассоциаций, союзов и иных объединений операторов, с учетом содержания персональных данных, характера и способов их обработки. 7. Проекты нормативных правовых актов, указанных в части 5 настоящей статьи, подлежат согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации. Проекты решений, указанных в части 6 настоящей статьи, подлежат согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в порядке, установленном Правительством Российской Федерации. Решение федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности, и федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации, об отказе в согласовании проектов решений, указанных в части 6 настоящей статьи, должно быть мотивированным. 8. Контроль и надзор за выполнением организационных и технических мер по обеспечению безопасности персональных данных, установленных в соответствии с настоящей статьей, при обработке персональных данных в государственных информационных системах персональных данных осуществляются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их	***соответствии с настоящим Федеральным законом требований по обеспечению безопасности персональных данных при их обработке для целей предоставления государственных и муниципальных услуг или исполнения иных государственных и муниципальных функций, осуществляется федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий и без права ознакомления с персональными данными, обрабатываемыми в информационных системах персональных данных.*** ***7. Операторы или объединения операторов, за исключением операторов, обрабатывающих персональные данные для целей предоставления государственных и муниципальных услуг или исполнения иных государственных и муниципальных функций, вправе применять национальный или международный стандарт обеспечения безопасности персональных данных при их обработке, либо разработать и утвердить собственный стандарт. Стандарты обеспечения безопасности персональных данных устанавливают меры по обеспечению безопасности персональных данных при их обработке в соответствии с частями 1 и 2 настоящей статьи.***	

полномочий и без права ознакомления с персональными данными, обрабатываемыми в информационных системах персональных данных. 9. Федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, и федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации, решением Правительства Российской Федерации с учетом значимости и содержания обрабатываемых персональных данных могут быть наделены полномочиями по контролю за выполнением организационных и технических мер по обеспечению безопасности персональных данных, установленных в соответствии с настоящей статьей, при их обработке в информационных системах персональных данных, эксплуатируемых при осуществлении определенных видов деятельности и не являющихся государственными информационными системами персональных данных, без права ознакомления с персональными данными, обрабатываемыми в информационных системах персональных данных. 10. Использование и хранение биометрических персональных данных вне информационных систем персональных данных могут осуществляться только на таких материальных носителях информации и с применением такой технологии ее хранения, которые обеспечивают защиту этих данных от неправомерного или случайного доступа к ним, их уничтожения, изменения, блокирования, копирования, предоставления, распространения. 11. Для целей настоящей статьи под угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их		

обработке в информационной системе персональных данных. Под уровнем защищенности персональных данных понимается комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.		
П. 2 ч. 2 ст. 22 2) полученных оператором в связи с заключением договора, стороной которого является субъект персональных данных, если персональные данные не распространяются, а также не предоставляются третьим лицам без согласия субъекта персональных данных и используются оператором исключительно для исполнения указанного договора и заключения договоров с субъектом персональных данных; **П. 4 ч. 2 ст. 22** 4) сделанных субъектом персональных данных общедоступными; **Ч. 4 ст. 22** 4. Уполномоченный орган по защите прав субъектов персональных данных в течение тридцати дней с даты поступления уведомления об обработке персональных данных вносит сведения, указанные в части 3 настоящей статьи, а также сведения о дате направления	**П. 2 ч. 2 ст. 22** 2) полученных оператором в связи ***намерением субъекта персональных данных заключить договор или*** с заключением договора, стороной которого ***или выгодоприобретателем*** является субъект персональных данных, если персональные данные не распространяются, а также не предоставляются третьим лицам без согласия субъекта персональных данных ***или иных оснований, установленных законодательством Российской Федерации*** и используются оператором исключительно для ***оценки возможности заключения указанного договора,*** исполнения указанного договора и ***(или)*** заключения ***новых*** договоров с субъектом персональных данных; **П. 4 ч. 2 ст. 22** 4) сделанных субъектом персональных данных ***или с согласия субъекта персональных данных*** общедоступными;	**П. 2, 4 ч. 2 ст. 22** Необходимо согласовать случаи обработки ПДн без согласия субъекта со случаями неуведомления уполномоченного органа в отношении различных форм обработки ПДн при договорных отношениях. **Ч. 4 ст. 22** Необходимо исключить публикацию в открытом доступе сведений о дислокации воинских частей, являющихся операторами ПДн, а также ПДн лиц, ответственных за обработку ПДн у оператора.

указанного уведомления в реестр операторов. Сведения, содержащиеся в реестре операторов, за исключением сведений о средствах обеспечения безопасности персональных данных при их обработке, являются общедоступными.	**Ч. 4 ст. 22** 4. Уполномоченный орган по защите прав субъектов персональных данных в течение тридцати дней с даты поступления уведомления об обработке персональных данных вносит сведения, указанные в части 3 настоящей статьи, а также сведения о дате направления указанного уведомления в реестр операторов. Сведения, содержащиеся в реестре операторов, за исключением сведений ***действительных наименованиях, подчиненности и месте дислокации воинских частей,*** о средствах обеспечения безопасности персональных данных при их обработке ***и персональных данных лица ответственного за организацию обработки персональных данных,*** являются общедоступными.	

ПРОЕКТ

РЕКОМЕНДАЦИИ

парламентских слушаний на тему: «Законодательное обеспечение прав субъектов персональных данных при их автоматизированной обработке»

Участники парламентских слушаний, рассмотрев вопрос о проекте федерального закона «О внесении изменений в Федеральный закон «О персональных данных», разработанном под руководством заместителя председателя Комитета по конституционному законодательству, правовым и судебным вопросам, развитию гражданского общества Р.У.Гаттарова на площадке Временной комиссии Совета Федерации по развитию информационного общества при участии экспертов из бизнес-структур и академических кругов, отмечают следующее.

Необходимость разработки проекта федерального закона обусловлена рядом факторов. Во-первых, основной российский закон в области защиты персональных данных - Федеральный закон от 27 июля 2006 года №152-ФЗ «О персональных данных» - был принят 7 лет назад и практика его применения выявила ряд недостатков. Во-первых, закон содержит ряд крайне сложных в реализации требований, что создает необоснованные барьеры в работе операторов персональных данных и толкает их на нарушения закона. В то же время для граждан избыточное регулирование закона порождает в большей степени неудобства, нежели действительно обеспечивает безопасность их персональных данных. Во-вторых, часть положений закона в настоящее время устарели или потеряли актуальность, а некоторые появившиеся за 7 лет аспекты работы с персональными данными он не регулирует вовсе. Фактически можно констатировать, что Федеральный закон №152-ФЗ «О персональных данных» более не обеспечивает адекватной защиты персональных данных, а также препятствует эффективной работе операторов персональных данных. На фоне быстрого роста количества персональных данных в электронном виде возникла

острая необходимость совершенствования законодательного регулирования в этой сфере и приведения его в соответствие с требованиями времени.

Существует неопределённость в правовом статусе лица, которое обрабатывает персональные данные по поручению оператора. Оператор персональных данных для поручения обработки данных другому лицу обязан получать согласие субъекта персональных данных, в то время как конструкция ответственности обеспечивает защиту прав субъектов персональных данных в таком случае. Для решения обозначенных проблем необходимо ввести понятие «субоператор персональных данных», определив его как лицо, осуществляющее обработку персональных данных по поручению оператора, предусмотрев в ряде случаев возможность поручать такую обработку без согласия физического лица.

Развитие электронных коммуникаций требует законодательного закрепления возможности дистанционного способа получения согласия субъекта на обработку его персональных данных. В связи с этим целесообразно законодательно предусмотреть возможность утверждения согласия на обработку персональных данных дистанционно, путем использования электронных средств, которые позволят оператору удостовериться в согласии конкретного лица на обработку его персональных данных. При этом необходимо уточнить, что на согласие в электронной форме не распространяются требования к согласию в письменной форме.

Одна из ключевых проблем в регулировании сферы заключается в том, что государственные органы, единожды получив письменное согласие субъекта на обработку его персональных данных, в дальнейшем осуществляют их обработку и передачу без получения дополнительного согласия и уведомления субъектов персональных данных, мотивируя это необходимостью предоставления государственных или муниципальных услуг. Для решения означенной проблемы необходимо:

- ограничить возможность органов власти обрабатывать персональные данные без согласия субъекта персональных данных только целями предоставления конкретной государственной или муниципальной услуги,

осуществления межведомственного взаимодействия, регистрации на федеральном и региональных порталах государственных и муниципальных услуг;

- ввести обязанность указанных операторов предоставлять субъектам персональных данных информацию об обработке их персональных данных в порядке, установленном для информирования о государственной или муниципальной услуге или иной государственной или муниципальной функции;

- конкретизировать исключение из правила об уведомлении уполномоченного органа об обработке персональных данных в составе государственных информационных систем.

Значимой проблемой для частных операторов является то, что требования к обеспечению безопасности персональных данных едины как для государственных, так и для частных операторов. Участникам слушаний представляется, что подходы к регулированию вопросов обеспечения безопасности персональных данных в публичных и частных информационных системах должны быть различными. Защиту персональных данных в публичных информационных системах необходимо осуществлять в соответствии с требованиями, устанавливаемыми уполномоченными Правительством Российской Федерации органами исполнительной власти, в частных - на основе международных или национальных стандартов по информационной безопасности.

Требует совершенствования законодательное регулирование трансграничной передачи персональных данных. В частности, необходимо расширить перечень оснований для трансграничной передачи персональных данных, если условия соглашения на обработку данных обеспечивают их адекватную защиту или если оператор персональных данных принял внутренние правила, которые обеспечивают такую защиту. Также необходимо ввести норму, согласно которой к основаниям сбора и обработки персональных данных, полученных и обработанных за пределами территории Российской Федерации, при обработке в Российской Федерации применяется не российское, а соответствующее иностранное законодательство.

Нуждается в конкретизации понятие «биометрические персональные данные». В настоящее время закон позволяет понимать под биометрическими данными в том числе и те данные, которые не используются операторами для установления личности физического лица. Следует внести изменения в законодательство, закрепив в понятийном аппарате понятие биометрических персональных данных как «биологических и поведенческих характеристик субъекта персональных данных, используемых для автоматической идентификации при установлении его личности».

Необходимо устранение имеющейся неопределённости в выборе норм законодательства при обработке персональных данных в составе иных конфиденциальных сведений. Для решения этой проблемы предлагается ввести разграничивающую норму. При этом персональные данные в составе сведений конфиденциального характера должны обрабатываться по требованиям специального законодательства, за исключением случаев, когда специальное законодательство не устанавливает требований к обработке данных.

На сегодняшний момент операторы персональных данных должны обеспечивать конфиденциальность персональных данных в отношении общедоступных и обезличенных персональных данных, а также в отношении данных, которые подлежат опубликованию или обязательному раскрытию в соответствии с федеральным законом. Это представляется излишним регулированием, в связи с чем необходимо закрепить положение о том, что конфиденциальность персональных данных в указанных случаях может не обеспечиваться.

Законодательством не установлен статус и требования к обработке идентификаторов сведений о физических лицах, используемых в публичном секторе. Для решения данной проблемы необходимо уточнить статью 13 Федерального закона «О персональных данных», предусмотрев, что способы обозначения принадлежности персональных данных в государственных и муниципальных информационных системах являются идентификаторами персональных данных. Также необходимо предусмотреть, что порядок и условия

использования идентификаторов персональных данных, а также требования по защите идентификаторов персональных данных, устанавливаются Правительством Российской Федерации.

Отмечая важность вышеуказанных проблем, связанных с совершенствованием законодательства в области защиты персональных данных и с учётом состоявшегося обсуждения участники парламентских слушаний рекомендуют:

поддержать проект федерального закона «О внесении изменений в Федеральный закон «О персональных данных», разработанный под руководством заместителя председателя Комитета по конституционному законодательству, правовым и судебным вопросам, развитию гражданского общества Р.У.Гаттарова на площадке Временной комиссии Совета Федерации по развитию информационного общества;

доработать проект федерального закона «О внесении изменений в Федеральный закон «О персональных данных» с учётом высказанных в ходе парламентских слушаний замечаний и предложений;

внести доработанный проект федерального закона в Государственную Думу Федерального Собрания Российской Федерации в соответствии со статьёй 104 Конституции Российской Федерации.