**Комиссия РСПП по связи и информационно-коммуникационным технологиям**

**ПРОЕКТ**

**Таблица изменений**

**к законопроекту № 101234-8 "О внесении изменений в Федеральный закон**

**«О персональных данных» и иные законодательные акты**

**Российской Федерации по вопросам защиты прав**

**субъектов персональных данных»**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **N/n** | **Часть, статья проекта** | **Редакция проекта** | **Предлагаемая редакция** | **Обоснование** |
| 1. | Подпункт “б” пункта 2 статьи 1 | б) в пункте 3 слова «передачу (распространение, предоставление, доступ)» заменить словами «передачу (распространение, предоставление), предоставление доступа или осуществление логических и (или) арифметических операций с такими данными,»; | Альтернативная редакция не предлагается, см. информацию в столбце “Обоснование”. | Редакция данной статьи выделяет такой способ обработки персональных данных как “доступ” из “передачи”. Однако в текст других норм Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных" (далее - “**Закон “О персональных данных**”) соответствующие поправки внесены не были. Это создает правовую коллизию и неопределенность правоприменительной практики. В частности, необходимы уточнения в ч. 5, 9, 11, 12, 14 ст. 10.1 “Особенности обработки персональных данных, разрешенных субъектом персональных данных для распространения” в части прав и обязанностей оператора и субъекта персональных данных. |
| 2. | Подпункт “в” пункта 2 статьи 1 | в) пункт 11 изложить в следующей редакции:  «11) трансграничная передача персональных данных – передача персональных данных **иностранному государству**, государственному органу иностранного государства, международной и иностранной организации, иностранному гражданину, лицу без гражданства **либо уполномоченному ими лицу**, юридическому лицу, зарегистрированному в иностранном государстве, или иной структуре без образования юридического лица независимо от их организационно-правовой формы, находящимся на территории иностранного государства.»; | в) пункт 11 изложить в следующей редакции:  «11) трансграничная передача персональных данных – передача персональных данных, государственному органу иностранного государства, международной и иностранной организации, иностранному гражданину, лицу без гражданства, юридическому лицу, зарегистрированному в иностранном государстве, или иной структуре без образования юридического лица независимо от их организационно-правовой формы, находящимся на территории иностранного государства.»; | Предлагаемая редакция статьи содержит в себе внутренние противоречия и создает коллизии с другими нормами Закона “О персональных данных”. Это влечет за собой правовую неопределенность и неоправданным образом усложняет бизнес-процессы.   1. Норма вступает в коллизию с предлагаемой редакцией ч. 1.1 ст. 1 Закона “О персональных данных”, поскольку **иностранное государство** не является субъектом, на которого распространяется действие Закона “О персональных данных”. Более того, наличие в перечне лиц, которым могут быть переданы персональные данные, иностранного государства в качестве самостоятельного субъекта является неоправданным, поскольку государство приобретает права и обязанности через свои государственные органы, которые отдельно названы в статье. В связи с этим отдельное упоминание иностранного государства вызовет непредсказуемость правоприменительной практики в связи с невозможностью однозначного толкования данной статьи (в такой редакции под трансграничную передачу персональных данных может попасть их передача российскому гражданину, временно находящемуся на территории иностранного государства). 2. Расширение нормы за счет **лица, уполномоченного иностранными лицами** является неоправданным, поскольку может привести к ограничению передачи персональных данных российским гражданам, находящимся на территории иностранных государств. В связи с этим предлагаемая редакция нормы содержит внутреннее противоречие, так как в отдельных случаях исключает критерий отсутствия российского гражданства из признаков трансграничной передачи персональных данных. |
| 3. | Подпункт “в” пункта 9 статьи 1 | в) дополнить частью 3 следующего содержания:  «3. Оператор не вправе отказывать в предоставлении услуг в случае отказа субъекта персональных данных предоставить биометрические персональные данные и(или) дать согласие на обработку персональных данных, если в соответствии с федеральным законом получение оператором согласия на обработку персональных данных не является обязательным. Предоставление биометрических персональных данных не может быть обязательным, за исключением случаев, предусмотренных в части 2 настоящей статьи.»; | Исключить положение | В настоящий момент Государственная Дума уже рассматривает законопроект, предметом регулирования которого является необоснованный запрос у потребителей персональных данных, получение которых не требуется для оказания услуг [(№ 1184356-7](https://sozd.duma.gov.ru/bill/1184356-7)), а также законопроект о внесении корреспондирующих изменений в КоАП РФ ([№ 1184517-7](https://sozd.duma.gov.ru/bill/1184517-7)). Принятие положений, дублирующих предмет регулирования указанных законопроектов, было бы избыточным. |
| 4. | Пункт 10 статьи 1 | 10) статью 12 изложить в следующей редакции:    "Статья 12. Трансграничная передача персональных данных    1. Трансграничная передача персональных данных осуществляется в соответствии с настоящим Федеральным законом.  2. Уполномоченный орган по защите прав субъектов персональных данных утверждает перечень иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных. В перечень иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных, включаются государства, являющиеся стороной Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, а также иные иностранные государства, не являющиеся стороной Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, при условии соответствия положениям указанной Конвенции действующих в соответствующем государстве норм права и применяемых мер по обеспечению конфиденциальности и безопасности персональных данных при их обработке.  3. Оператор до начала осуществления деятельности по трансграничной передаче персональных данных обязан уведомить уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять трансграничную передачу персональных данных.  4. Уведомление, предусмотренное частью 3 настоящей статьи, направляется в виде документа на бумажном носителе или в форме электронного документа и подписывается уполномоченным лицом. Уведомление о намерении осуществлять трансграничную передачу персональных данных должно содержать следующие сведения:  1) наименование (фамилия, имя, отчество), адрес оператора;  **2) источник(и) получения персональных данных;**  3) правовое основание и цель трансграничной передачи и дальнейшей обработки переданных персональных данных;  4) категории и перечень передаваемых персональных данных;  5) категории субъектов персональных данных, персональные данные которых передаются;  **6) сведения о государственном органе, муниципальном органе, юридическом или физическом лице, которому планируется передача персональных данных, в том числе его контактная информация;**  **7) сведения о принимаемых государственным органом, муниципальным органом, юридическим или физическим лицом, которому планируется трансграничная передача персональных данных, мерах по защите передаваемых персональных данных и условиях прекращения их обработки;**  **8) информация о правовом регулировании в области персональных данных иностранного государства, под юрисдикцией которого находится государственный орган, муниципальный орган, юридическое или физическое лицо, которому планируется передача персональных данных (в случае, если предполагается осуществление трансграничной передачи персональных данных государственному органу, муниципальному органу, юридическому или физическому лицу, находящемуся под юрисдикцией иностранного государства, не включенного в перечень иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных).**  5. Трансграничная передача персональных данных может быть запрещена или ограничена в целях защиты основ конституционного строя Российской Федерации, нравственности, здоровья, прав и законных интересов граждан,обеспечения обороны страны и безопасности государства.  6. Решение о запрещении или ограничении трансграничной передачи персональных данных в целях защиты нравственности, здоровья, прав и законных интересов граждан принимается уполномоченным органом по защите прав субъектов персональных данных по результатам рассмотрения уведомления оператора о намерении осуществлять трансграничную передачу персональных данных.  7. Решение о запрещении или ограничении трансграничной передачи персональных данных в целях защиты основ конституционного строя Российской Федерации и безопасности государства принимается уполномоченным органом по защите прав субъектов персональных данных по представлению федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности.  8. Решение о запрещении или ограничении трансграничной передачи персональных данных в целях обеспечения обороны страны принимается уполномоченным органом по защите прав субъектов персональных данных по представлению федерального органа исполнительной власти, уполномоченного в области обороны.  **9. Решение о запрещении или ограничении трансграничной передачи персональных данных в целях защиты экономических и финансовых интересов Российской Федерации принимается уполномоченным органом по защите прав субъектов персональных данных по представлению федеральных органов исполнительной власти, уполномоченных Президентом Российской Федерации, Правительством Российской Федерации.**  10. Решение о запрещении или ограничении трансграничной передачи персональных данных принимается уполномоченным органом по защите прав субъектов персональных данных в течение тридцати дней с даты поступления уведомления, предусмотренного частью 3 настоящей статьи, в порядке, установленном Правительством Российской Федерации.  11. При рассмотрении уполномоченным органом по защите прав субъектов персональных данных в рамках тридцатидневного срока уведомления оператора о своем намерении осуществлять трансграничную передачу персональных данных на территорию иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных, возможность оператора осуществлять трансграничную передачу персональных данных на территорию указанных иностранных государств не ограничивается.  **12. При рассмотрении уполномоченным органом по защите прав субъектов персональных данных в рамках тридцатидневного срока уведомления оператора о своем намерении осуществлять трансграничную передачу персональных данных на территорию иностранных государств, не обеспечивающих адекватную защиту прав субъектов персональных данных, трансграничная передача персональных данных на территорию указанных иностранных государств оператором не допускается.**  13. В случае, принятия решения, предусмотренного частью **10** настоящей статьи, оператор обязан обеспечить уничтожение государственным органом, муниципальным органом, юридическим или физическим лицом ранее переданных ему персональных данных." | Исключить положения  В качестве **альтернативного варианта**, если исключить положения представится невозможным по публично-правовым основаниям:  10) статью 12 изложить в следующей редакции:    "Статья  12. Трансграничная передача персональных данных    1. Трансграничная передача персональных данных осуществляется в соответствии с настоящим Федеральным законом.  2. Уполномоченный орган по защите прав субъектов персональных данных утверждает перечень иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных. В перечень иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных, включаются государства, являющиеся стороной Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, а также иные иностранные государства, не являющиеся стороной Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, при условии соответствия положениям указанной Конвенции действующих в соответствующем государстве норм права и применяемых мер по обеспечению конфиденциальности и безопасности персональных данных при их обработке.  3. Оператор до начала осуществления деятельности по трансграничной передаче персональных данных обязан уведомить уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять трансграничную передачу персональных данных.  4. Уведомление, предусмотренное частью 3 настоящей статьи, направляется в виде документа на бумажном носителе или в форме электронного документа и подписывается уполномоченным лицом. Уведомление о намерении осуществлять трансграничную передачу персональных данных должно содержать следующие сведения:  **1) наименование (фамилия, имя, отчество), адрес оператора;**  **2) правовое основание и цель трансграничной передачи и дальнейшей обработки переданных персональных данных;**  **3) категории и перечень передаваемых персональных данных;**  **4) категории субъектов персональных данных, персональные данные которых передаются.**  5. Трансграничная передача персональных данных может быть запрещена или ограничена в целях защиты основ конституционного строя Российской Федерации, нравственности, здоровья, прав и законных интересов граждан,обеспечения обороны страны и безопасности государства.  6. Решение о запрещении или ограничении трансграничной передачи персональных данных в целях защиты нравственности, здоровья, прав и законных интересов граждан принимается уполномоченным органом по защите прав субъектов персональных данных по результатам рассмотрения уведомления оператора о намерении осуществлять трансграничную передачу персональных данных.  7. Решение о запрещении или ограничении трансграничной передачи персональных данных в целях защиты основ конституционного строя Российской Федерации и безопасности государства принимается уполномоченным органом по защите прав субъектов персональных данных по представлению федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности.  8. Решение о запрещении или ограничении трансграничной передачи персональных данных в целях обеспечения обороны страны принимается уполномоченным органом по защите прав субъектов персональных данных по представлению федерального органа исполнительной власти, уполномоченного в области обороны.  **8.** Решение о запрещении или ограничении трансграничной передачи персональных данных принимается уполномоченным органом по защите прав субъектов персональных данных в течение тридцати дней с даты поступления уведомления, предусмотренного частью 3 настоящей статьи, в порядке, установленном Правительством Российской Федерации.  **9.** При рассмотрении уполномоченным органом по защите прав субъектов персональных данных в рамках тридцатидневного срока уведомления оператора о своем намерении осуществлять трансграничную передачу персональных данных на территорию иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных, возможность оператора осуществлять трансграничную передачу персональных данных на территорию указанных иностранных государств не ограничивается.  **10.** При рассмотрении уполномоченным органом по защите прав субъектов персональных данных в рамках тридцатидневного срока уведомления оператора о своем намерении осуществлять трансграничную передачу персональных данных на территорию иностранных государств, не обеспечивающих адекватную защиту прав субъектов персональных данных, **трансграничная передача персональных данных на территорию указанных иностранных государств оператором 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.**  **11.** В случае, принятия решения, предусмотренного частью **8** настоящей статьи, оператор обязан обеспечить уничтожение государственным органом, муниципальным органом, юридическим или физическим лицом ранее переданных ему персональных данных." | 1. Предлагаемая норма значительно осложнит деятельность интернет-компаний, что противоречит мерам поддержки IT-отрасли в 2022 году, инициированным Президентом и Правительством РФ. Среди таких мер – освобождение компаний отрасли от различных видов государственного контроля или упрощение такого контроля, снижение числа проверочных мероприятий.   Поскольку Интернет является глобальной сетью, подавляющее большинство интернет-компаний так или иначе осуществляет трансграничную передачу персональных данных. Например, сотрудники для работы с компьютерными устройствами используют **системное программное обеспечение** Windows (поддержку обеспечивает компания Microsoft Corp.), Linux (поддержку обеспечивает компания IBM Corp.), macOS (поддержку обеспечивает компания Apple Inc.), в рамках взаимодействия с которыми возможна трансграничная передача данных - для устранения возникших технических ошибок, общения со службой технической поддержки, кастомизации программ под потребности российских компаний. Помимо этого, при работе сайтов неизбежно использование **cookie-файлов**, без которых работа сайтов станет невозможной или существенно затруднится, уменьшится защищенность информации. Это сделает российские сайты менее конкурентоспособными.  В то же время обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну, является целью российского законодательства о персональных данных, поэтому обеспечение конфиденциальности персональных данных является не менее важным общественным интересом.  Одновременно необходимо отметить, что **текущее регулирование уже обладает достаточными механизмами** для защиты персональных данных в случае их передачи за рубеж:   * операторы до начала обработки персональных данных обязаны уведомлять Роскомнадзор об осуществлении трансграничной передачи персональных данных, конкретных государствах, а также правовых основаниях, целях обработки и категориях обрабатываемых персональных данных (п. 2, 3, 5, 10 ч. 3 ст. 22 Закона “О персональных данных”); * Роскомнадзор имеет право ограничить или запретить передачу персональных данных на территорию иностранных государств в целях защиты основ конституционного строя Российской Федерации, нравственности, здоровья, прав и законных интересов граждан, обеспечения обороны страны и безопасности государства (ч. 1 ст. 12 Закона “О персональных данных”; * возможность передачи персональных данных на территорию иностранных государств, которыми не обеспечивается адекватная защита прав субъектов персональных данных уже ограничены и возможна только в конкретных случаях (информированное согласие субъекта персональных данных, необходимость исполнения заключенного по волеизъявлению субъекта персональных данных договора (*например, в случае приобретения авиабилетов или бронирования гостиничного номера*); выполнение обязанностей по законодательству (*например, для международной регистрации патента на изобретение, товарного знака, получения сертификата соответствия ЕАЭС) - ч. 4 ст. 12 Закона “О персональных данных”;* * осуществление оператором трансграничной передачи персональных данных является основанием для повышения категории риска и более частого проведения Роскомнадзором плановых контрольных мероприятий (Постановление Правительства РФ от 29.06.2021 N 1046 "О федеральном государственном контроле (надзоре) за обработкой персональных данных").   В связи с этим предлагаемое регулирование является избыточным и соответствующие положения **целесообразно исключить.** Они существенным образом затруднят деятельность российских компаний, сделают их сервисы менее конкурентоспособными и инновационными, и при это не способны достичь заявленную цель по повышению уровня защищенности персональных данных граждан - по сравнению с механизмами, которые уже есть в наличии у Роскомнадзора согласно текущему законодательству.     1. В качестве **альтернативного варианта**, в случае если изменение регулирования трансграничной передачи персональных данных по публично-правовым основаниям будет расценено как необходимое, считаем, что предложенные изменения регулирования трансграничной передачи персональных данных **потребуют корректировки**, чтобы избежать неоправданного усложнения условий деятельности операторов. 2. Требования к содержанию уведомления о намерении осуществлять трансграничную передачу персональных данных являются избыточными и обременительными для операторов. Из них необходимо **исключить** следующие сведения:  * **источник(и) получения персональных данных** (поскольку из нормы неясно, в какой форме указывать такие сведения; если сведения получены от пользователей интернет-сервиса оператора, нужно ли указывать ФИО всех субъектов персональных данных и т.п.); * **сведения о государственном органе, муниципальном органе, юридическом или физическом лице, которому планируется передача персональных данных, в том числе его контактная информация** (поскольку такая информация является избыточной с точки зрения обеспечения прав субъектов персональных данных); * **сведения о принимаемых государственным органом, муниципальным органом, юридическим или физическим лицом, которому планируется трансграничная передача персональных данных, мерах по защите передаваемых персональных данных и условиях прекращения их обработки** (поскольку полный перечень таких мер может быть неизвестен оператору); * **информацию о правовом регулировании в области персональных данных иностранного государства, под юрисдикцией которого находится государственный орган, муниципальный орган, юридическое или физическое лицо, которому планируется передача персональных данных (в случае, если предполагается осуществление трансграничной передачи персональных данных государственному органу, муниципальному органу, юридическому или физическому лицу, находящемуся под юрисдикцией иностранного государства, не включенного в перечень иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных)** - поскольку в соответствии с частью 2 статьи 12 (в редакции проекта) именно уполномоченный орган по защите прав субъектов персональных данных утверждает перечень иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных. Если иностранное государство не было включено в перечень иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных, то уполномоченному органу по защите прав субъектов персональных данных априори известно как о причинах принятия такого решения, так и о правовом регулировании в области персональных данных соответствующего иностранного государства.  1. В части 5 статьи 12 (в редакции законопроекта) указан **закрытый** перечень оснований, по которым может быть запрещена или ограничена трансграничная передача персональных данных, повторяющий текст **части 3 статьи 55 Конституции РФ**. Защита экономических и финансовых интересов Российской Федерации не является основанием для ограничения прав и свобод человека и гражданина федеральным законом**. Таким образом, часть 9 статьи 12 в редакции законопроекта противоречит Конституции РФ.** 2. Частью 12 статьи 12 (в редакции законопроекта) устанавливается, что если оператор намерен осуществлять трансграничную передачу персональных данных на территорию иностранных государств, не обеспечивающих адекватную защиту прав субъектов персональных данных, то такой оператор не вправе осуществлять такую передачу в период рассмотрения уполномоченным органом по защите прав субъектов персональных данных уведомления оператора в рамках тридцатидневного срока.   Указанная ситуация необоснованным образом обременяет деятельность оператора, например, **в части организации командировок работников** в иностранные государства, не обеспечивающие адекватную защиту прав субъектов персональных данных. В случае принятия нормы работодатель будет ограничен в возможности заблаговременно приобрести авиабилеты и провести иные организационные мероприятия.  Полагаем, что даже в период рассмотрения уполномоченным органом по защите прав субъектов персональных данных уведомления оператора о намерении осуществлять трансграничную передачу персональных данных на территорию иностранных государств, не обеспечивающих адекватную защиту прав субъектов персональных данных, оператор должен иметь возможность осуществлять такую передачу **в случаях, которые в действующей редакции части 4 ст. 12 Закона “О персональных данных” установлены как предоставляющие оператору право осуществлять трансграничную передачу персональных данных на территорию иностранных государств, не обеспечивающих адекватную защиту прав субъектов персональных данных.** Это наличие согласия в письменной форме субъекта персональных данных и т.п. |
| 5. | Абзац третий подпункта “б” пункта 11 статьи 1 | “1.2. В течение тридцати дней с даты получения оператором соответствующего требования субъекта персональных данных оператор обязан прекратить их обработку и (или) принять меры по их уточнению, блокированию, уничтожению, либо направить субъекту персональных данных мотивированный отказ в случае, если обработка персональных данных осуществляется в соответствии с пунктами 1-5, 8 части 1 статьи 6 настоящего закона.»; | Исключить положения | 1. Данная норма проекта создает правовую коллизию с другими положениями Закона “О персональных данных” и вызывает правовую неопределенность для операторов и правоприменительных органов относительно того, какая из норм закона подлежит применению в конкретном случае, т.е. какие действия и в какие сроки обязан предпринять оператор.   Так, обязанность оператора прекратить обработку персональных данных по требованию субъекта персональных данных и принять соответствующие меры уже содержится в действующей редакции Закона “О персональных данных”:   * часть 1 статьи 21 закона закрепляет обязанность оператора по обращению субъекта персональных данных блокировать персональные данные в случае их неточности или неправомерной обработки; * часть 2 статьи 21 закона закрепляет обязанность оператора уточнить персональные данные в течение 7 дней с даты представления сведений; * часть 3 статьи 21 закона закрепляет обязанность оператора прекратить неправомерную обработку в течение 3 дней с даты ее выявления, при невозможности - уничтожить данные в течение 10 дней; * часть 4 статьи 21 закона закрепляет обязанность оператора по достижении целей прекратить обработку персональных данных и уничтожить их в течение 30 дней.   Наличие таких коллизий делает регуляторную среду непредсказуемой, а также создает необоснованные препятствия в ведении бизнеса в связи с угрозой необоснованного привлечения к административной ответственности по усмотрению конкретных сотрудников правоприменительных органов. Данное обстоятельство также является коррупциогенным фактором.   1. Предложенная норма **фактически ухудшает положение субъекта персональных данных и уменьшает объем защиты его прав**, поскольку статья 21 Закона “О персональных данных” предусматривает более короткие сроки реагирования на обращение субъекта персональных данных, а также предполагает принятие определенных мер (блокирование, уничтожение персональных данных), не оставляя это на усмотрение самого оператора. 2. Предложенная норма содержит правовую коллизию с часть 4 статьи 21 Закона “О персональных данных”, а также предложенной проектом редакцией части 5.1 статьи 21 Закона “О персональных данных”.   Предложенная норма предусматривает исключения только в отношении определенных правовых оснований обработки персональных данных в соответствии с частью 1 статьи 6 закона, в то время как:   * корреспондирующая ей часть 5.1 статьи 21 закона содержит исключения для случаев обработки персональных данных по всем иным правовым основаниям в соответствии с частью 1 статьи 6, частью 2 статьи 10 и частью 2 статьи 11 закона. * часть 4 статьи 21 закона предусматривает право оператора продолжить обработку персональных данных в соответствии с иными правовыми основаниями, закрепленными Законом “О персональных данных” и иными федеральными законами.   Данные противоречия создают правовую неопределенность относительно того, в каких именно случаях оператор обязан прекратить обработку персональных данных по требованию субъекта персональных данных, а в каких – имеет право направить мотивированный отказ в связи с отсутствием нарушения Закона “О персональных данных”. Наличие подобной коллизии пагубно отразится на бизнес-процессах операторов и создает основания для необоснованного усмотрения сотрудников правоприменительных органов.   1. **Отсутствие в исключениях, позволяющих продолжить обработку персональных данных, пунктов 7, 9 и 11 части 1 статьи 6** Закона “О персональных данных” является необоснованным, поскольку в законе отсутствует иерархия правовых оснований обработки персональных данных. В свою очередь, предложенная норма безосновательным образом придает согласию субъекта персональных данных большую юридическую силу, чем, например, достижению общественно значимых целей, ведению исследовательской деятельности, обработке данных, подлежащих обязательному опубликованию на основании федерального закона. Это может привести не только к нарушению бизнес-процессов компаний (**невозможности проводить научные, в т.ч. социологические исследования, например для урбанистических целей**), но также и невозможности обеспечить безопасность сотрудников и сохранность собственности компаний, пресечение правонарушений (**в случае поступления требования лица удалить в качестве “устаревших” данные с публичных видеокамер компании, зафиксировавших его недобросовестные действия**). |
| 6. | Подпункт “в” пункта 11 статьи 1 | в) в части 3 слова "при обращении либо при получении" заменить словами "в течение**десяти** рабочих дней с момента обращения, либо получения оператором", дополнить следующим предложением: "Оператор предоставляет сведения, указанные в части 7 настоящей статьи субъекту персональных данных или его представителю в той форме, в которой направлено соответствующее обращение либо запрос, если иное не указано в самом обращении или запросе." | в) в части 3 слова "при обращении либо при получении" заменить словами "в течение **тридцати**дней с момента обращения, либо получения оператором", дополнить следующим предложением: "Оператор предоставляет сведения, указанные в части 7 настоящей статьи субъекту персональных данных или его представителю в той форме, в которой направлено соответствующее обращение либо запрос, если иное не указано в самом обращении или запросе." | 1. Сокращение срока предоставления операторами информации по запросам субъектов персональных данных создаст дополнительную нагрузку на бизнес, особенно в условиях нестабильной экономической ситуации, а также неоправданным образом ограничит возможность исследовать все обстоятельства дела и представить наиболее полный, подробный ответ, отражающий все детали сложившейся ситуации. Операторы также будут вынуждены понести расходы на дополнительный наём и оплату труда работников, обеспечивающих организацию и рассмотрение обращений. Указанное **противоречит мерам поддержки IT-отрасли в 2022 году, инициированным Президентом РФ.**      1. Текущий срок в 30 дней является оправданным, так как позволяет при подготовке ответа использовать детализированный подход к сбору информации, учесть все технические, операционные и юридические аспекты и получить требуемую информацию от различных бизнес-направлений и департаментов компаний, технических специалистов. 2. 30-дневный срок предоставления информации в сфере обработки персональных данных является стандартной практикой в различных юрисдикциях, в т.ч. предусмотрен Общим регламентом по защите персональных данных Европейского Союза (GDPR). |
| 7. | Пункт 15 статьи 1 | 15) статью 19 дополнить частями 12 - 14 следующего содержания:  "12. Оператор обязан в порядке, определенном федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, о**беспечивать непрерывное взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, включая информирование о компьютерных инцидентах, повлекших неправомерные доступ, представление, распространение, передачу персональных данных.**  **13. Указанная в части 12 настоящей статьи информация (за исключением информации, составляющей государственную тайну) передается федеральным органом, уполномоченным в области обеспечения безопасности в федеральный орган исполнительной власти, осуществляющий функции по контролю (надзору) за соответствием обработки персональных данных.**  **14. Порядок передачи информации в соответствии с частью 13 настоящей статьи устанавливается совместно федеральным органом, уполномоченным в области обеспечения безопасности и федеральным органом исполнительной власти, осуществляющим функции по контролю (надзору) за соответствием обработки персональных данных."** | 15) статью 19 дополнить частями 12 - 14 следующего содержания:  "12. Оператор обязан в порядке, определенном федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, **информировать федеральный орган исполнительной власти, осуществляющий функции по контролю (надзору) за соответствием обработки персональных данных**, о компьютерных инцидентах, повлекших неправомерные доступ, предоставление, распространение персональных данных (за исключением информации, составляющей государственную тайну).  **13.** **Оператор, получивший в установленном законом порядке право на проведение работ с использованием сведений, составляющих гостайну, обязан в порядке, определенном федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, обеспечивать непрерывное взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, включая информирование о компьютерных инцидентах, повлекших неправомерные доступ, представление, распространение, передачу персональных данных.** | 1. Порядок взаимодействия ГосСОПКА с различными органами и организациями предусмотрен Федеральным законом от 26.07.2017 N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». Этот закон распространяется на критическую информационную инфраструктуру и её субъекты, под которыми в первую очередь понимаются владельцы информационной инфраструктуры в ограниченном количестве сфер: здравоохранение, наука, транспорт, связь, энергетика, банки и финансовый рынок, топливно-энергетический комплекс, атомная энергия, оборонная, ракетно-космическая, горнодобывающая, металлургическая и химическая промышленность.  Распространение обязанности взаимодействия с ГосСОПКА на практически неограниченно широкий круг организаций приведёт к коллизиям между регулированием Закона “О персональных данных” и Федерального закона от 26.07.2017 N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».  Помимо этого, для организации такого взаимодействия **операторам потребуется понести расходы** на приобретение оборудования, его отладку и запуск, а также на оплату труда работников, которые будут выполнять соответствующие функции. При этом возможность компенсации расходов операторов проектом не предусмотрена.  Указанный порядок **противоречит концепции мер поддержки IT-отрасли в 2022 году, инициированных Президентом и Правительством РФ.** 2. Законопроект не устанавливает **вид нормативно-правового акта**, которым должны быть введены нормы, **детализирующие порядок непрерывного взаимодействия операторов с ГосСОПКА**, и государственный орган, уполномоченный принять такой акт. Сам законопроект таких норм не содержит, что уже само по себе создаёт пробел в регулировании. 3. Из действующей редакции Закона “О персональных данных” следует, что каждая организация является оператором персональных данных. В настоящий момент в Российской Федерации зарегистрировано около 7 млн. юридических лиц и ИП. Миллионы новых одновременных подключений в автоматическом режиме к одной и той же информационной системе не могут не оказать негативного влияния на стабильность каналов связи.  Таким образом, предложенный механизм повлечёт за собой **многократное увеличение нагрузки на информационную инфраструктуру интернет-провайдеров**, что приведёт к перебоям с доступностью интернет-сервисов и убыткам для компаний отрасли. 4. В качестве **альтернативы введению обязанности для всех операторов обеспечить взаимодействие с ГосСОПКА** предлагаем обязать всех операторов **направлять уведомления о компьютерных инцидентах,** повлекших неправомерные доступ, предоставление, распространение, персональных данных, **непосредственно в**  **федеральный орган исполнительной власти, осуществляющий функции по контролю (надзору) за соответствием обработки персональных данных** (за исключением информации, составляющей государственную тайну). 5. Отдельное перечисление таких способов обработки персональных данных, как “представление” и “распространение” создает правовую коллизию с определением “передачи персональных данных”, устанавливаемым подпунктом “б” пункта 2 статьи 1 проекта: “передача” включает в себя предоставление и распространение. Это создает правовую неопределенность и избыточную дискретность правоприменения относительно содержания термина “передача” персональных данных, используемого, в частности, в положениях Закона “О персональных данных”, касающихся обработки персональных данных, разрешенных субъектом персональных данных для распространения, трансграничной передачи персональных данных, (статьи 10.1, 12 Закона), и при этом не способно усилить защиту персональных данных. 6. Для операторов, получивших право на проведение работ с использованием сведений, составляющих государственную тайну, предлагаем установить обязанность обеспечить взаимодействие с ГосСОПКА. |
| 8. | Пункт 16 статьи 1 | 16) в статье 20:  а) в части 1 слова "тридцати дней" заменить словами "десяти рабочих дней";  б) в части 2 слова "тридцати дней" заменить словами "десяти рабочих дней";  в) в части 4 слова "тридцати дней" заменить словами "десяти рабочих дней" | Исключить положение | Аналогично изложенному для строки 6 настоящей таблицы. |
| 9. | Подпункт “г” пункта 17 статьи 1 | г) дополнить частью 31 следующего содержания:  «31. В случае установления факта неправомерного или случайного доступа, **предоставления, распространения, передачи** персональных данных, повлекших нарушение прав субъектов персональных данных оператор обязан **в течение двадцати четырех часов с момента наступления такого инцидента** уведомить уполномоченный орган по защите прав субъектов персональных данных. Указанная информация должна содержать **сведения о причинах, повлекших нарушение прав субъектов персональных данных,** о предполагаемом вреде, нанесенном правам субъектов персональных данных, **о лицах, допустивших указанный доступ**, а также о принятых мерах по устранению соответствующих последствий.»; | г) дополнить частью 31 следующего содержания:  «31. В случае установления факта неправомерного или случайного доступа, **предоставления, распространения** персональных данных, повлекших нарушение прав субъектов персональных данных оператор обязан в течение **трех рабочих дней с момента выявления такого инцидента** уведомить уполномоченный орган по защите прав субъектов персональных данных. Указанная информация должна содержать сведения о **предполагаемых** причинах, повлекших нарушение прав субъектов персональных данных, о предполагаемом вреде, нанесенном правам субъектов персональных данных, а также о принятых мерах по устранению соответствующих последствий.»; | Устанавливаемая предлагаемой нормой обязанность уведомлять Роскомнадзор об инцидентах с персональными данными является **фактически нереализуемой для операторов.**   1. Обязанность уведомлять Роскомнадзор в течение двадцати четырех часов **с момента наступления инцидента фактически невыполнима** - оператор может выявить инцидент не в момент его происшествия, а спустя определенный промежуток времени (*например, если бумажный документ, содержащий персональные данные, был направлен не тому адресату*). Вместо этого предлагается уведомлять Роскомнадзор **с момента выявления инцидента**. 2. Срок уведомления Роскомнадзора в двадцать четыре часа является неоправданно коротким и его соблюдение **фактически невозможно операторами.** Например, если инцидент произошел во время выходных или нерабочих праздничных дней. Более того, норма предполагает предоставление Роскомнадзору определенного набора сведений об инциденте, а не только информирование о факте его возникновения. Сбор таких данных требует участия различных бизнес-направлений и департаментов оператора, получения сведений от технических специалистов, всестороннего анализа обстоятельств дела. Проведение указанной работы в течение двадцати четырех часов крайне затруднительна, а в ряде случаев принципиально невозможна. В связи с этим текущая редакция нормы автоматически сделает такого оператора виновным в нарушении срока уведомления Роскомнадзора об инциденте и повлечет его привлечение к административной ответственности. Это создает дополнительную, неоправданную нагрузку на бизнес и **противоречит мерам поддержки IT-отрасли в 2022 году, инициированным Президентом РФ.** 3. Согласно текущей редакции нормы уведомление должно включать в себя информацию, в том числе о причинах возникновения инцидента, а также о конкретных лицах, допустивших его возникновение. **Предоставление такой информации в короткий срок является фактически невозможным для оператора.** Достоверное выявление причин возникновения инцидента, связанного с неправомерным или случайным доступом, предоставлением или распространением персональных данных третьим лицам, требует установления всех обстоятельств дела, длительного и детализированного расследования, определения мотивов и умысла действия конкретных лиц, изучения бизнес и технологических процессов компании, их исследования на предмет возможных уязвимостей, исследования независимыми компаниями, имеющими лицензиями в сфере обеспечения конфиденциальности информации, достаточности ранее принятых компанией мер в сфере информационной безопасности. Уведомление может содержать только сведения о **предполагаемых причинах**. Аналогичным образом, в течение короткого промежутка времени невозможно установление виновных лиц. Их выявление в большинстве случаев находится в зоне ответственности правоохранительных органов, имеющих полномочия и специализированные средства для установления личностей виновников происшествий - например, **в случае хакерской атаки на информационные системы оператора**. 4. Отдельное перечисление таких способов обработки персональных данных как “представление” и “распространение” создает правовую коллизию с определением “передачи персональных данных”, устанавливаемым подпунктом “б” пункта 2 статьи 1 проекта: “передача” включает в себя предоставление и распространение. Это создает правовую неопределенность и избыточную дискретность правоприменения относительно содержания термина “передача” персональных данных, используемого, в частности, в положениях Закона “О персональных данных”, касающихся обработки персональных данных, разрешенных субъектом персональных данных для распространения, трансграничной передачи персональных данных, (ст. 10.1, 12 Закона), и при этом не способно усилить защиту персональных данных. |
| 10. | Подпункт “ж” пункта 17 статьи 1 | ж) дополнить частью 5.1 следующего содержания:  «5.1. В случае обращения субъекта персональных данных к оператору с требованием о прекращении обработки персональных данных оператор обязан в срок, не превышающий тридцати дней с момента обращения либо получения оператором соответствующего требования прекратить их обработку или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется лицом, осуществляющим обработку персональных данных) за исключением случаев, предусмотренных в пунктах 2 - 11 части 1 статьи 6, части 2  статьи 10 и части 2 статьи 11 настоящего Федерального закона.»; | Исключить положения | 1. Данная норма проекта создаёт правовую коллизию с другими положениями Закона “О персональных данных” и вызывает правовую неопределенность для операторов и правоприменительных органов относительно того, какая из норм закона подлежит применению в конкретном случае, т.е. какие действия и в какие сроки обязан предпринять оператор.   Так, обязанность оператора прекратить обработку персональных данных по требованию субъекта персональных данных и принять соответствующие меры уже содержится в действующей редакции Закона “О персональных данных”:   * ч. 1 ст. 21 закона закрепляет обязанность оператора по обращению субъекта персональных данных блокировать персональные данные в случае их неточности или неправомерной обработки; * ч. 2 ст. 21 закона закрепляет обязанность оператора уточнить персональные данные в течение 7 дней с даты представления сведений; * ч. 3 ст. 21 закона закрепляет обязанность оператора прекратить неправомерную обработку в течение 3 дней с даты ее выявления, при невозможности - уничтожить данные в течение 10 дней; * ч. 4 ст. 21 закона закрепляет обязанность оператора по достижении целей прекратить обработку персональных данных и уничтожить их в течение 30 дней.   Наличие таких коллизий делает регуляторную среду непредсказуемой для операторов, а также создает необоснованные препятствия в ведении бизнеса в связи с наличием угрозы необоснованного привлечения к административной ответственности по усмотрению конкретных сотрудников правоприменительных органов. Данное обстоятельство также является коррупциогенным фактором.   1. Предложенная норма **фактически ухудшает положение субъекта персональных данных и уменьшает объем защиты его прав**, поскольку ч. 1, 2, 3, 4 ст. 21 Закона “О персональных данных” предусматривают более короткие сроки реагирования на обращение субъекта персональных данных, а также предполагает принятие определенных мер (блокирование, уничтожение персональных данных), не оставляя это на усмотрение самого оператора. 2. Предложенная норма содержит правовую коллизию с ч. 4 ст. 21 Закона “О персональных данных”, предусматривающей право оператора продолжить обработку персональных данных в соответствии с правовыми основаниями, закрепленными не только Законом “О персональных данных”, но и иными федеральными законами.   Данные противоречия создают правовую неопределенность относительно того, в каких именно случаях оператор обязан прекратить обработку персональных данных по требованию субъекта персональных данных, а в каких имеет право направить мотивированный отказ в связи с отсутствием нарушения норм Закона “О персональных данных”. Наличие подобной коллизии пагубно отразится на бизнес-процессах операторов и создает основания для личного необоснованного усмотрения сотрудников правоприменительных органов. |
| 11. | Абзац второй подпункт “а” пункта 18 статьи 1 | пункты 1 - 6 признать утратившими силу; | Исключить положения | Норма законопроекта исключает практически все (кроме двух) случаи, когда операторы вправе обрабатывать персональные данные без уведомления уполномоченного органа по защите прав субъектов персональных данных.   1. Норма вступает в противоречие с мерами поддержки IT-отрасли в 2022 году, которые инициированы Президентом и Правительством РФ и направлены на освобождение компаний отрасли от отдельных обязанностей, установленных законами. 2. Поскольку все организации в своей деятельности обрабатывают персональные данные, новелла приведёт к практически полному совпадению по субъектному составу ЕГРЮЛ/ЕГРИП и Реестра операторов, осуществляющих обработку персональных данных, что ставит вопрос о целесообразности отдельного существования этих реестров. 3. Нахождение записи об операторе в Реестре операторов, осуществляющих обработку персональных данных, в любом случае не влияет на порядок осуществления в отношении оператора федерального государственного контроля за обработкой персональных данных в соответствии с Законом “О персональных данных” и Постановлением Правительства РФ от 29.06.2021 N 1046 "О федеральном государственном контроле (надзоре) за обработкой персональных данных". |
| 12. | Абзац второй подпункта “б” пункта 18 статьи 1 | пункты 3 - 6 признать утратившими силу; | Исключить положения | Аналогично изложенному для строки 13 настоящей таблицы. |
| 13. | Подпункт “в” пункта 18 статьи 1 | в) дополнить частью 31 следующего содержания:  «31. При предоставлении сведений, предусмотренных частью 3 настоящей статьи, оператор для каждой цели обработки персональных данных указывает: категории персональных данных, категории субъектов, персональные данные которых обрабатываются, правовое основание обработки персональных данных, перечень действий с персональными данными, способы обработки персональных данных.»; | Исключить положение | 1. Норма увеличит объём текста уведомления, который операторы направляют в уполномоченный орган по защите прав субъектов персональных данных в соответствии со ст. 22 Закона “О персональных данных”, что приведёт к дополнительным трудозатратам со стороны работников операторов и – как следствие – увеличению расходов операторов. 2. Норма противоречит мерам поддержки IT-отрасли в 2022 году, инициированным Президентом и Правительством РФ, которые в т.ч. направлены на содействие компаниям отрасли в сложный экономический период. Помимо этого, в результате реализации указанной нормы Реестр операторов, осуществляющих обработку персональных данных станет содержать значительное количество дублирующих сведений. |
| 14. | Абзац третий подпункта “г” пункта 19 статьи 1 | 11. Информация, содержащаяся в указанном реестре, о компьютерных инцидентах, повлекших неправомерные доступ, **представление, распространение, передачу** персональных данных, в порядке, установленном совместно федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности и федеральным органом исполнительной власти, осуществляющим функции по контролю (надзору) за соответствием обработки персональных данных, передается в федеральный орган исполнительной власти, уполномоченным в области обеспечения безопасности.». | 11. Информация, содержащаяся в указанном реестре, о компьютерных инцидентах, повлекших неправомерные доступ, **предоставление, распространение** персональных данных, в порядке, установленном совместно федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности и федеральным органом исполнительной власти, осуществляющим функции по контролю (надзору) за соответствием обработки персональных данных, передается в федеральный орган исполнительной власти, уполномоченным в области обеспечения безопасности.». | Предлагаемая редакция данной нормы создает правовую коллизию с определением “передачи персональных данных”, устанавливаемым подпунктом “б” пункта 2 статьи 1 проекта, согласно которому **передача включает в себя предоставление и распространение**.  Отдельное перечисление таких способов обработки персональных данных как “представление” и “распространение” вместе с включающей их “передачей” создает правовую неопределенность и избыточную дискретность правоприменения относительно содержания термина “передача” персональных данных, используемого, в частности, в положениях Закона “О персональных данных”, касающихся обработки персональных данных, разрешенных субъектом персональных данных для распространения, трансграничной передачи персональных данных, (ст. 10.1, 12 Закона), и при этом не способно усилить защиту персональных данных. |
| 15. | Пункт 2 статьи 2 | 2) дополнить статьей 36.3 следующего содержания:  Статья 36.3.  Правила внесения в Единый государственный реестр недвижимости записи о возможности предоставления персональных данных правообладателя объекта недвижимости, содержащихся в Едином государственном реестре недвижимости    …  8. Запись, указанная в части 1 настоящей статьи, погашается на основании:  1) представленного в порядке, предусмотренном частью 4 настоящей статьи, заявления гражданина, указанного в части 1 настоящей статьи, об отзыве ранее представленного заявления о возможности предоставления третьим лицам сведений о его фамилии, имени и отчестве;  2) вступившего в законную силу судебного акта, обязывающего орган регистрации прав погасить данную запись. | Исключить положения | 1. Поправки, направленные на ограничение доступа лиц, совершающих запросы о предоставлении сведений, содержащихся в ЕГРН, к сведениям о фамилии, имени, отчестве и дате рождения физического лица, за которым в ЕГРН зарегистрировано право, ограничение права или обременение на соответствующий объект недвижимости (далее – “**правообладатель**”), **усложнят оборот объектов недвижимости** (что станет ещё более неблагоприятным обстоятельством в сложной экономической ситуации), а также могут привести к **увеличению случаев мошенничества** виду усложнения доступа для граждан к значимой информации в отношении объектов недвижимости. 2. К настоящему моменту в Федеральном законе от 13.07.2015 N 218-ФЗ “О государственной регистрации недвижимости” уже содержатся нормы, устанавливающие ограничение доступа к сведениям о правообладателях, содержащимся в ЕГРН:  * Предоставление сведений из ЕГРН регулируется статьей 62 Федерального закона от 13.07.2015 N 218-ФЗ «О государственной регистрации недвижимости». Частью 13 статьи установлено, что некоторые наиболее чувствительные сведения из содержащихся в ЕГРН (обобщенные сведения о правах отдельного лица на имеющиеся или имевшиеся у него объекты недвижимости, сведения о признании правообладателя недееспособным или ограниченно дееспособным и др.) **могут быть предоставлены лишь ограниченному перечню заявителей**. Среди них сами правообладатели, их законные представители и представители по доверенности, руководители и заместители руководителей государственных органов, суды, правоохранительные органы, судебные приставы и подобные субъекты. Соответственно, **не приходится говорить о возможности любого лица произвольно получить сведения о другом лице из ЕГРН.** * В 2021 году статья 62 Федерального закона от 13.07.2015 N 218-ФЗ “О государственной регистрации недвижимости” была дополнена частями 1.1. и 1.2., которые были в том числе направлены на защиту персональных данных правообладателей. В результате было специально закреплено, что **персональные данные правообладателей нельзя размещать на официальном сайте Росреестра в открытом доступе**. В случае принятия уполномоченными органами решений о наложении **запрета на выдачу сведений о защищаемых лицах и их близких, объектах государственной охраны и членах их семей, сведения о таких лицах, содержащиеся в ЕГРН, не предоставляются**, за исключением случаев, предусмотренных федеральными законами либо указом Президента Российской Федерации.      1. В указанных нормах содержится юридико-технические ошибки: в статье 2 проекта содержатся две различные нормы, обозначенные пунктами “2”; помимо них, присутствуют ещё две различные нормы, обозначенные подпунктами “ж”, в рамках одного из пунктов “2”.      1. В предлагаемых проектом поправках присутствуют положения, которые заслуживают поддержки. Среди них: указание, что сведения, содержащиеся в ЕГРН, являются общедоступными в пределах, установленных законом; установление необходимости предъявлять нотариально удостоверенную доверенность в целях получения обобщенных сведений о правах отдельного лица на имеющиеся или имевшиеся у него объекты недвижимости; выведение единой информационной системы нотариата из-под действия запрета, установленного частью 27.1 статьи 62 Федерального закона от 13.07.2015 N 218-ФЗ “О государственной регистрации недвижимости”. |
| 16. | Подпункт “а” пункта 2 статьи 2 | дополнить частью 1.3 следующего содержания:  "1.3. Сведения, содержащиеся в Едином государственном реестре недвижимости и представляющие собой персональные данные о правообладателе объекта недвижимости (лицом, в пользу которого зарегистрированы ограничения права или обременения объекта недвижимости), относятся к сведениям, доступным с согласия правообладателя объекта недвижимости третьим лицам, только при наличии в Едином государственном реестре недвижимости записи, указанной в статье 36.3 настоящего Федерального закона." |
| 17. | Подпункт “б” пункта 2 статьи 2 | б) часть 7 дополнить предложением следующего содержания: "В случае если правообладателем объекта недвижимости является гражданин, которым в соответствии со статьей 36.3 настоящего Федерального закона в Единый государственный реестр недвижимости в орган регистрации прав не подавалось заявление о внесении записи о возможности предоставления персональных данных правообладателя объекта недвижимости, в указанную в настоящей части выписку из Единого государственного реестра недвижимости включаются сведения о принадлежности данного объекта физическому лицу без указания персональных данных правообладателя, установленных в части 1 статьи 36.3 настоящего Федерального закона, за исключением случаев, когда указанные сведения запрашиваются лицами, указанными в части 6 статьи 36.3 настоящего Федерального закона." |
| 18. | Подпункт “в” пункта 2 статьи 2 | в) дополнить частью 8.1 следующего содержания:  "8.1. Выписка из Единого государственного реестра недвижимости, содержащая персональные данные правообладателя объекта недвижимости, установленные в части 1 статьи 36.3 настоящего Федерального закона, может быть проверена любым лицом посредством официального сайта на предмет действительности содержащейся в ней информации о правообладателе указанного в ней объекта недвижимости на дату выдачи такой выписки с предоставлением ему и правообладателю результата такой проверки, имеющего уникальный идентификационный номер." |
| 19. | Подпункт “г” пункта 2 статьи 2 | г) в части 13:  **абзац первый после слов "реестре недвижимости," дополнить словами "представляющие собой персональные данные лица, за которым в Едином государственном реестре недвижимости зарегистрировано право, ограничение права или обременение объекта недвижимости,"**;  пункт 2 после слов "лицам, имеющим" дополнить словами "нотариально удостоверенную" | г) в части 13:  пункт 2 после слов "лицам, имеющим" дополнить словами "нотариально удостоверенную". | Аналогично изложенному для строк 15-18 настоящей таблицы. |
| 20. | Подпункт “д” пункта 2 статьи 2 | д) дополнить частью 14.1 следующего содержания:  "14.1. Сведения, содержащие персональные данные правообладателя объекта недвижимости… …  …если таким лицам указанные сведения необходимы для совершения сделки с объектом недвижимости." | Исключить положения |
| 21 | Подпункт “ж” пункта 2 статьи 2 | ж) [дополнить](https://login.consultant.ru/link/?req=doc&base=LAW&n=411575&dst=100799&field=134&date=14.04.2022) частью 27.2 следующего содержания:  "27.2. Запрет, предусмотренный [частью 24 настоящей статьи](https://login.consultant.ru/link/?req=doc&base=LAW&n=411575&dst=640&field=134&date=14.04.2022)… …  …которому такие сведения необходимы для защиты прав и законных интересов." |
| 22. | Статья 3 | Статья 3    Внести в Основы законодательства Российской Федерации о нотариате от 11 февраля 1993 года N 4462-1 (Ведомости Съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации, 1993, N 10, ст. 357; Собрание законодательства Российской Федерации, 2004, N 45, ст. 4377; 2011, N 49, ст. 7064; 2012, N 41, ст. 5531; 2013, N 51, ст. 6699; 2014, N 30, ст. 4268; 2015, N 1, ст. 10; N 13, ст. 1811; 2016, N 1, ст. 11; N 27, ст. 4293; 2018, N 22, ст. 3043) следующие изменения:  …  2. По письменному совместному заявлению правообладателя объекта недвижимости и иного заинтересованного лица нотариусом запрашиваются содержащиеся в Едином государственном реестре недвижимости сведения о фамилии, имени, отчестве и дате рождения гражданина - правообладателя объекта недвижимости в виде выписки из данного реестра в случае, если таким лицам указанные сведения необходимы для совершения сделки с объектом недвижимости. Наличие указанных сведений нотариус удостоверяет свидетельством." |