DOI: http://dx.doi.org/10.21686/2411-118X-2022-3-56-61

Основные тенденции правового регулирования персональных данных в России и Европейском союзе и их влияние на бизнес

А. Д. Фролова
юрист ООО «ГлоуБайт Аналитические Решения»
Адрес: ООО «ГлоуБайт Аналитические Решения»,
119530, Москва, внутригородские муниципальные образования Москвы,
Муниципальный Округ Очаково-Матвеевское, ш. Очаковское, д. 28, строение 2.
E-mail: 21039595@mail.ru

The Main Trends in the Legal Regulation of Personal Data in Russia and the European Union and Their Impact on Business

A. D. Frolova
Lawyer of LLC “GlowByte Analytical Solutions”
Address: LLC “GlowByte Analytical Solutions”
28, Building 2, Ochakovskoye Highway, Inner-City Municipalities of Moscow,
The Municipal District of Ochakovo-Matveevskoye, Moscow, 119530, Russian Federation.
E-mail: 21039595@mail.ru

Аннотация

В статье рассматриваются основные положения Общего регламента по защите персональных данных (далее – GDPR) и Федерального закона № 152 «О персональных данных» (далее – ФЗ-152) как основных источников правового регулирования сферы персональных данных в России и Европейском союзе. Проводится сравнительно-правовой анализ норм Регламента и ФЗ-152 с учетом изменений, внесенных в закон. Подчеркивается высокий уровень развития законодательного регулирования GDPR в вопросах обеспечения безопасности обработки персональных данных, прав субъектов персональных данных, а также во взаимодействии участников процесса обработки данных с надзорными органами. Особое внимание уделяется механизмам защиты персональных данных, оцениваются возможные последствия и их влияние на бизнес в рамках внесенных изменений в ФЗ-152. Делается вывод о том, что инициированные поправки к закону в значительной степени направлены на обеспечение прав и интересов субъектов персональных данных, но в то же время могут вызвать усложнение процессов для бизнеса.

Ключевые слова: субъект персональных данных, оператор, контролер, процессор, лицо, осуществляющее обработку персональных данных, защита персональных данных.

Abstract

This article discusses the main provisions of the General Data Protection Regulation (next – GDPR) and Federal Law № 152 "On Personal Data" (next – Law-152) as the main sources of legal regulation of the sphere of personal data in Russia and the European Union. A comparative legal analysis of some rules of the Regulation and Law-152 is carried out, taking into account the changes proposed in the new draft law. The high level of development of GDPR standards in matters of ensuring the security of personal data processing, the rights of personal data subjects, as well as in the interaction of participants in the data processing process with supervisory authorities is emphasized. Particular attention is paid to the mechanisms of personal data protection, the possible consequences and their impact on business within the framework of the amendments to law-152. It is concluded that the initiated amendments to the law are largely aimed at ensuring the rights and interests of personal data subjects, but at the same time may cause complication of processes for business.

Keywords: personal data subject, operator, controller, processor, person processing personal data, personal data protection.

На сегодняшний день проблема правовой охраны персональных данных является актуальной как в России, так и за рубежом в связи с массовым распространением информации и персональных данных субъектов.

Основным законом, нацеленным на урегулирование персональных данных в России, является Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее – ФЗ-152)[1]. В соответствии с законом «персональные данные – это любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу». Таким образом, перечень персональных данных не конкретизируется законодателем, оставляя этот список открытым.

В Европейском союзе (далее – ЕС) регулирование персональных данных осуществляется с помощью Общего регламента по защите персональных данных (The Regulation (EU) 2016/679 (General Data Protection Regulation – далее – GDPR или Регламент)[2]. Определение персональных данных в этом документе практически не отличается от представленного в ФЗ-152: «любая информация, связанная с определенным или определяемым физическим лицом («субъектом данных»). Определяемое лицо признается таковым, если оно может быть определено прямо или косвенно, в частности, посредством ссылки на его имя, идентификационный номер и т. п.»

Относительно участников процесса обработки персональных данных в ФЗ-152 и Регламенте употребляются практически одинаковые термины с разницей в их наименованиях. GDPR под процессором понимает лицо, осуществляющее обработку персональных данных (есть и в российском законе).

Совсем недавно в статье 3 ФЗ-152 «О персональных данных» не было указано определение понятия «лица, осуществляющего обработку персональных данных», но недавний Законопроект от 6 апреля 2022 г. № 101234-8 «О внесении изменений в Федеральный закон «О персональных данных» и иные законодательные акты Российской Федерации по вопросам защиты прав субъектов персональных данных» (далее – законопроект) ввел это понятие, подчеркнув, что, в отличие от оператора, лицо, занимающееся обработкой персональных данных, не определяет цели обработки персональных данных, их состав. В качестве контролера GDPR определяет физическое или юридическое лицо, которое само определяет цели и средства обработки персональных данных. Такое определение соответствует оператору в ФЗ-152.

Ранее ФЗ-152 имел юридическую силу только на территории России, в отличие от GDPR, который носит экстерриториальный характер. Однако законопроект внес изменения, чтобы распространить действие настоящего закона вне территории России[3]. Пока непонятно, каким образом уполномоченные органы будут вмешиваться в работу с персональными данными российских граждан на территории иностранных государств тем не менее такие поправки к закону уже приняты.

Несмотря на то что Регламент является продуктом нормотворчества ЕС, нормы GDPR могут распространяться за пределы ЕС, в том числе и на российские юридические лица. Это вытекает из самого текста Регламента, а именно статьи 3, где определяется сфера действия Регламента и критерии его применения:

1) если оператор или обработчик, который совершает действия с персональными данными, осуществляет предпринимательскую деятельность на территории ЕС. При этом не имеет значения, где именно он обрабатывают персональные данные[4];

2) если оператор не имеет присутствия на территории ЕС и данный оператор обрабатывает

[1] Федеральный закон от 27 июля 2006 г. № 152-ФЗ (ред. от 2 июля 2021 г.) «О персональных данных» // Собрание законодательства Российской Федерации. – 2006. – № 31 (часть 1). – Статья 3451.

[2] The Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). – URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>

[3] Законопроект от 6 апреля 2022 г. № 101234-8 «О внесении изменений в Федеральный закон «О персональных данных» и иные законодательные акты Российской Федерации по вопросам защиты прав субъектов персональных данных». – URL: < https://sozd.duma.gov.ru/bill/101234-8>

[4] Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD), CJEU, C-131/12. – URL: < https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A 62012CJ0131>; Unabhängiges Landeszentrum für Datenschutz Schleswig- Holstein/Wirtschaftsakademie Schleswig-Holstein GmbH, CJEU C-210/16. – URL: < https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62016C J0210>

данные субъекта, находящегося на территории ЕС. Это условие применяется в отношении товаров или услуг, которые предлагаются субъектам, проживающим на территории ЕС, или в связи с мониторингом поведения лиц, находящихся на территории ЕС. Однако стоит отметить, что если такие товары или услуги предоставляются случайно или непостоянно на территории ЕС, то к данной ситуации Регламент не будет применим [4].

Во всех случаях применения GDPR, указанных в статье 3 Регламента, организация, не зарегистрированная в ЕС, должна назначить представителя в ЕС. При этом в данном требовании есть исключения. Представитель может быть не назначен, если:

1) обработка носит временный характер;

2) специальные категории персональных данных не обрабатываются в больших объемах;

3) обработка не нарушает права и свободы физических лиц;

4) обработку персональных данных осуществляют государственные органы.

Представителем может быть физическое или юридическое лицо, которое должно находиться в одном из государств, где присутствуют субъекты, чьи персональные данные обрабатываются, и которое уполномочено контролером или процессором. Однако принципиальным является тот факт, что последние по-прежнему остаются ответственными за свои действия.

ФЗ-152 предусматривает возможность трансграничной передачи персональных данных, т. е. передачу персональных данных на территорию иностранных государств. До принятия поправок к Федеральному закону одним из условий трансграничной передачи была обязанность оператора убедиться, что иностранное государство, на территорию которого передаются персональные данные, способно обеспечить адекватную защиту прав субъектов персональных данных до начала трансграничной передачи персональных данных. Теперь после принятия вышеупомянутого законопроекта оператору будет вменяться обязанность уведомлять уполномоченный орган о такой передаче. Уведомление должно содержать наименование оператора; источник, из которого получены персональные данные; цель трансграничной передачи и их дальнейшей обработки; категорию субъектов персональных данных, чьи данные передаются; сведения о государственном органе, юридическом или физическом лице, которому планируется передача данных; сведения о мерах, которые принимаются государственными органами, лицами, получающими персональные данные.

В уведомлении также необходимо указать информацию о том, какими законами регулируется сфера персональных данных в иностранном государстве, под юрисдикцией которого находится лицо, которому планируется передать персональные данные. Однако данную информацию следует указывать в случае, если трансграничная передача осуществляется лицу, которое находится в государстве, не способном обеспечить адекватную защиту субъектов персональных данных.

Таким образом, помимо общей информации, трансграничную передачу которой оператор должен будет направить в уполномоченный орган путем уведомления, ему придется провести анализ правового регулирования персональных данных иностранным государством, в которое он планирует передавать персональные данные. Сбор такой информации также накладывает на компании дополнительные финансовые и трудовые затраты.

При этом не имеет значения, в какое иностранное государство оператор будет направлять персональные данные – государство, которое является стороной Конвенции Совета Европы «О защите физических лиц при автоматизированной обработке персональных данных» (далее – Конвенция), либо в государство, которое не ратифицировало данную Конвенцию.

Трансграничную передачу персональных данных можно запретить или ограничить в целях защиты основ и безопасности государства, нравственности, здоровья и прав граждан этого государства. В принятом законопроекте отдельно указано, что в то время, как уполномоченный орган будет рассматривать уведомление оператора о трансграничной передаче персональных данных на территорию иностранного государства, способного обеспечить защиту персональных данных субъекта, осуществлять трансграничную передачу на территорию указанного иностранного государства можно без ограничений, т. е. оператор может выполнять действия по трансграничной передаче одновременно с принятием решения уполномоченным органом.

Трансграничная передача запрещается на территорию иностранных государств, которые не обеспечивают защиту персональных данных

субъектов до тех пор, пока уполномоченный орган не примет положительное решение.

Кроме того, в случае запрета или ограничения трансграничной передачи оператору следует обеспечить уничтожение лицом ранее переданных им персональных данных. При этом оператор должен отчитываться о любой трансграничной передаче персональных данных в уполномоченный орган. Такой подход кажется не вполне рациональным по причине того, что это может затруднить работу бизнеса, в частности IT-компаний, работающих с облачным сервисом.

В европейском законодательстве под трансграничной передачей понимается передача персональных данных для их обработки в третью страну или международную организацию. Однако важным условием такой передачи является то, что она возможна только при условии соблюдения условий Регламента.

Если Европейская комиссия решит, что третья страна способна обеспечить адекватный уровень защиты персональных данных, то никакого специального разрешения на трансграничную передачу не потребуется. Однако комиссия в любой момент может изменить свое решение, если обнаружит, что законодательство третьей страны не отвечает установленным критериям обеспечения защиты. Тем не менее шанс передать персональные данные даже в страны, которые не могут обеспечить надлежащий уровень защиты, имеется, если контролер и процессор дадут гарантии, и при условии, что у субъектов персональных данных есть эффективные средства правовой защиты.

Стоит также упомянуть изменения закона, касающиеся случаев обработки персональных данных, при которых не требуется уведомлять уполномоченный орган. До вступления поправок к ФЗ-152 в силу их было перечислено девять, но с принятием законопроекта их количество существенно сократилось.

Таким образом, теперь не уведомлять уполномоченный орган можно только в случае: если такие персональные данные включены в государственные информационные системы для защиты безопасности государства; если обработка персональных данных осуществляется без использования средств автоматизации; персональные данные обрабатываются в целях соблюдения законодательства о транспортной безопасности. Такое сокращение случаев неуведомления уполномоченного органа видится избыточным. Поскольку важно не только усилить контрольные меры, но и обеспечить понятный и удобный для всех участников процесс.

Европейский Регламент предусматривает достаточно много возможностей для осуществления субъектом контроля за своими персональными данными. Субъект персональных данных имеет право получить доступ к своим данным, касающимся цели обработки, информации о получателях данных, сроке хранения и т. д. Субъект также имеет право на удаление и изменение своих персональных данных, отзыв согласия на обработку персональных данных, ограничение обработки. Относительно недавно в GDPR появилось право субъекта на перенос персональных данных от одного контролера другому. ФЗ-152 в свою очередь предусматривает практически те же вышеупомянутые права субъекта персональных данных, что и GDPR, кроме права на перенос персональных данных.

Положения о мерах защиты персональных данных субъектов при их обработке достаточно подробно получили свое развитие в GDPR. Регламент содержит подробный план взаимодействия участников процесса обработки персональных данных с надзорными органами. Причем важной особенностью является то, что такое сотрудничество происходит еще до начала действий с персональными данными.

Регламент предусматривает необходимость анализа воздействия на защиту данных в случае, если происходит обработка специальных категорий данных или компания проводит постоянный мониторинг субъектов. При этом если существует большая вероятность, что такой вид обработки, особенно с использованием новых технологий, ставит под риск права и интересы субъектов, то оценка воздействия определенно необходима.
Такая оценка должна включать в себя цели обработки (соотношение необходимости обработки с ее целями), предполагаемую оценку рисков для прав субъекта, меры, которые планируется принять для устранения рисков.

Отдельной мерой по защите персональных данных является назначение инспектора. На роль инспектора назначается лицо, владеющее экспертными знаниями законов о персональных данных.

Существуют обязательные случаи, когда контролер или процессор обязан назначать инспектора:

1) обработка осуществляется государственным органом, за исключением судов;

2) происходит постоянный мониторинг деятельности субъектов;

3) специальные категории персональных данных обрабатываются в большом количестве.

Основными задачами инспектора являются информирование и консультирование контролера или процессора по вопросам, связанным с персональными данными, осуществление мониторинга соблюдения Регламента и других законов, связанных с персональными данными, предоставление рекомендаций по оценке воздействия защиты персональных данных, сотрудничество с надзорными органами.

При этом инспектор несет ответственность перед высшим руководством контролера и процессора. Поэтому инспектор не получает от контролера и процессора никаких инструкций при осуществлении своей деятельности и не может быть ими уволен. Таким образом, обеспечивается равенство интересов и дополнительный контроль за обеспечением прав и свобод субъектов.

В дополнение к вышеперечисленным мерам Регламент приветствует принятие контролерами и процессорами различных кодексов поведения, учреждение механизмов сертификации. Помимо превентивных мер, GDPR содержит порядок действий в случае нарушения безопасности персональных данных.

Так, контролер обязан уведомить надзорный орган в течение семидесяти двух часов после обнаружения незаконного доступа к персональным данным. В свою очередь Регламент обязывает процессора уведомлять контролера немедленно без неоправданной задержки. Такое уведомление должно содержать характер нарушения, по возможности количество пострадавших субъектов, описание последствий, предпринятые или предлагаемые к принятию меры для устранения такого нарушения.

Законодательное регулирование обеспечения безопасности персональных данных в России также не стоит на месте. Внесенные поправки в ФЗ-152 направлены на совершенствование мер по их защите. Статья 18.1 ФЗ-152 предусматривает, какие меры оператор мог принять для выполнения своих обязанностей. Поправки к Федеральному закону сделали эти меры обязательными для оператора, сохранив за ним возможность самостоятельно определять состав и перечень таких мер.

Еще одним нововведением стала обязанность оператора наладить взаимодействие с государственной системой, связанной с предотвращением компьютерных атак. В случае возникновения неправомерного доступа к персональным данным субъекта оператор обязан в течение двадцати четырех часов с момента наступления такого инцидента сообщить об этом уполномоченному органу. Сам уполномоченный орган будет вести реестр учета таких инцидентов.

Проблема защиты персональных данных субъектов является краеугольным камнем в вопросе их регулирования. Законодательство обязано учитывать те вызовы и проблемы, которые возникают сегодня в сфере охраны персональных данных. Как в ЕС, так и в России наблюдается довольно быстрое развитие законодательного регулирования. GDPR имеет большую проработанность в вопросах предотвращения незаконного доступа к персональным данным и их утечки. В то же время нельзя принижать роль ФЗ-152, поскольку он достаточно проработан в этих вопросах.

С принятием поправок к ФЗ-152 появилось много существенных изменений в трансграничной передаче, уведомлении уполномоченного органа об обработке персональных данных, а также укрепилось взаимодействие операторов с уполномоченными органами с целью защиты персональных данных.

Безусловно, все эти меры призваны обеспечить соблюдение прав субъектов персональных данных и сократить количество незаконного доступа к их персональным данным. В то же время важным является недопущение учинения препятствий бизнесу в их деятельности в связи с ужесточением законодательства в области персональных данных, которое, вероятно, еще претерпит множество изменений.

Список литературы

1. *Абышко А. О.* Конец общедоступных персональных данных в России? К вопросу о Федеральном законе от 30 декабря 2020 года N 519-ФЗ // Закон. 2022. N 3.

2. *Грибанов А. А*. Общий регламент о защите персональных данных (General Data Protection Regulation) : идеи для совершенствования российского законодательства // Закон. – 2018. – С. 149–162.

3. *Нам К. В*. Особенности развития правового регулирования оборота и защиты персональных данных // Вестник гражданского права. 2020. N 5.

4. *Савельев А. И.* Научно-практический постатейный комментарий к Федеральному закону «О персональных данных». – М. : Статут, 2017.

5. *Савельев А. И.* Гражданско-правовые аспекты регулирования оборота данных в условиях попыток формирования цифровой экономики // Вестник гражданского права. – 2020. – № 1. – С. 60–92.

6. *Солдатова В. И.* Проблемы защиты персональных данных в условиях применения цифровых технологий // Право и экономика. – 2019. – № 12.