Сравнительная характеристика GDPR и российского законодательства о персональных данных

И. С. Денисов
кандидат юридических наук, доцент кафедры гражданско-правовых дисциплин
РЭУ им. Г. В. Плеханова.
Адрес: ФГБОУ ВО «Российский экономический университет имени Г. В. Плеханова», 117997, Москва, Стремянный пер., д. 36.
E-mail: is.denisov@mail.ru

Д. Р. Ахматова
студентка 3-го курса факультета экономики и права
РЭУ им. Г. В. Плеханова.
Адрес: ФГБОУ ВО «Российский экономический университет имени Г. В. Плеханова», 117997, Москва, Стремянный пер., д. 36.
E-mail: akhmatova.dzhamilya@mail.ru

В. М. Кабакова
студентка 3-го курса факультета экономики и права
РЭУ им. Г. В. Плеханова.
Адрес: ФГБОУ ВО «Российский экономический университет имени Г. В. Плеханова», 117997, Москва, Стремянный пер., д. 36.
E-mail: vkabakova@list.ru

Comparative Characteristics of the GDPR and Russian Legislation on Personal Data

I. S. Denisov
PhD in Law, Associate Professor of the Department of Civil Legal Disciplines of the PRUE.
Address: Plekhanov Russian University of Economics, 36 Stremyanny Lane, Moscow, 117997, Russian Federation.
E-mail: is.denisov@mail.ru

D. R. Akhmatova
Third-Year Student of the Faculty of Economics and Law of the PRUE.
Address: Plekhanov Russian University of Economics, 36 Stremyanny Lane, Moscow, 117997, Russian Federation.
E-mail: akhmatova.dzhamilya@mail.ru

V. M. Kabakova
Third-Year Student of the Faculty of Economics and Law of the PRUE.
Address: Plekhanov Russian University of Economics, 36 Stremyanny Lane, Moscow, 117997, Russian Federation.
E-mail: vkabakova@list.ru

Аннотация

В данной статье рассмотрены основные причины разработки и внедрения Общего регламента по защите данных (General Data Protection Regulation, GDPR) Европейского союза, заменившего собой Директиву 95/46/EC (Data Protection Directive), принятую в 1995 г., выявлена актуальность применения данного регламента в российской практике. Методология работы основана на сравнительном анализе GDPR и Федерального закона № 152 «О персональных данных», благодаря чему были сделаны выводы об общих чертах и различиях основных положений. Научную новизну исследования определяют предложения авторов,

направленные на совершенствование законодательства, регулирующего проблемы защиты и обработки персональных данных. Возможность применения требований GDPR рассмотрена на конкретных примерах, что позволило выявить определенные критерии, которые показывают, что деятельность организации осуществляется в сфере действия GDPR. В заключение предлагаются пять этапов внедрения принципов GDPR в деятельность организации для наиболее эффективной работы с данными и соблюдения законодательства. Также в работе были рассмотрены некоторые спорные решения, связанные с обработкой персональных данных в российской и зарубежной практике на примере таких организаций, как «ВКонтакте», Facebook, Google, ICANN и EPAG.

Ключевые слова: персональные данные, конфиденциальность, цифровизация, информация, обработка данных, защита данных, GDPR, интернет, информационные технологии, контроль, анализ, регламент, процессор, контроллер, ЕС.

Abstract

This article examines the main reasons for the development and implementation of the General Data Protection Regulation (GDPR) of the European Union, which replaced the EU Data Protection Directive 95/46 adopted in 1995. In this article authors defined the relevance of the application of these regulations in the Russian practice. The methodology of the work is based on a comparative analysis of the GDPR and the Federal Law No. 152 “On personal data”, due to which conclusions about the general features and differences of the main provisions were made. The scientific novelty of the study is determined by the authors' proposals aimed at improving the legislation regulating the problems of protection and processing of personal data. The possibility of applying the provisions of the GDPR is considered on specific examples, which made it possible to identify certain criteria that show that the organization’s activities are carried out in the scope of the GDPR. In conclusion, five stages of introducing the principles of GDPR into the organization’s activities are proposed for the most efficient work with data and compliance with legislation. Also, some controversial decisions related to the processing of personal data in Russian and foreign practice were considered on the example of such organizations as VKontakte, Facebook, Google, ICANN and EPAG.

Keywords: personal data, confidentiality, digitalization, information, data processing, data protection, GDPR, Internet, information technology, control, analysis, regulations, processor, controller, EU.

Стремительное развитие технологий и глобализация породили новые проблемы в области защиты персональных данных. С этой целью европейские органы власти приняли решение создать прочную и согласованную систему защиты данных в Европейском союзе (ЕС).

В январе 2012 г. Европейская комиссия предложила новую реформу о защите персональных данных. Ее цель заключалась в том, чтобы вернуть гражданам контроль за своими данными, в то же время упростив нормативную среду бизнеса.

После четырех лет законодательных переговоров и около четырех тысяч поправок текст был окончательно принят Европейским парламентом 14 апреля 2016 г. Это положение получило название «Общие правила защиты данных», или General Data Protection Regulation (GDPR), заменило Директиву 95/46/ЕС (Data Protection Directive), принятую в 1995 г., и вступило в силу 25 мая 2018 г. [1].

GDPR преследует три основные цели:

1) укрепление прав физических лиц, данные которых используются;

2) определение ответственности всех сторон, занимающихся обработкой данных;

3) обеспечение доверия к регулированию данных в рамках цифрового суверенитета посредством расширения сферы применения санкций в случае невыполнения правил регламента [7. – С. 222].

Требования GDPR обязаны соблюдать не все компании, а только те, которые обрабатывают персональные данные резидентов и граждан ЕС. GDPR имеет экстерриториальное действие, т. е. местонахождение организации не имеет значения: она может быть как на территории ЕС, так и за ее пределами. Субъектами GDPR являются контроллеры и процессоры.

Контроллеры – это компании или организации, которые собирают данные пользователей.

Процессоры – компании, которые их обрабатывают от имени контроллеров.

Внедрение GDPR стало революционным шагом в сфере защиты информации и было встречено критикой. Многие противники GDPR считают нововведения административным бременем для стран ЕС. Однако на сегодняшний день все

больше компаний используют в своей деятельности стандарты GDPR.

Российские компании также проявляют интерес к новым стандартам защиты и обработки персональных данных. Так, Сбербанк России рассчитывает инвестировать 1 млн долларов в новые технологии защиты данных. Другие российские компании, такие как «Банк ВТБ», ОАО «РЖД», ПАО «Лукойл», также готовятся к внедрению европейского регламента [6].

Данная тенденция во многом обусловлена снижением доверия людей к обеспечению конфиденциальности их данных. Так, 85% покупателей не станут приобретать товар у компании, если посчитают ее недостаточно безопасной, а 61% может отказаться от транзакций из-за положений политики безопасности [9. – С. 5]. Данная статистика связана с ростом нарушений конфиденциальности информации.

Исследование показало, что на сегодняшний день особо острой является проблема кражи цифровой личности, к основным элементам которой относят историю посещений сайтов, геолокацию, данные в облачном хранилище и др.

В российской практике аналогом GDPR является Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных». Во многих вопросах Федеральный закон № 152 схож с GDPR. Так, можно выделить общие принципы обработки данных:

– законность процессов обработки персональных данных;
– справедливость процессов обработки персональных данных;
– понятность процессов гражданину;
– точность и актуальность данных;
– обработка только для заявленных целей;
– отсутствие избыточных данных;
– ограниченный срок сохранения;
– сохранность и конфиденциальность [9. – С. 14].

Рассматривая права субъектов, можно также выделить общие элементы:

– доступ к данным и информации об обработке;
– корректировка и дополнение данных;
– уничтожение данных (право на забвение);
– блокировка обработки данных;
– возражение против обработки данных;
– отзыв согласия.

Также имеются существенные различия в правах субъектов.

GDPR устанавливает дополнительные права для защиты персональных данных, которые могут быть рассмотрены в качестве рекомендации для совершенствования Федерального закона № 152:

– перенос данных (data portability right);
– получение копии данных (raw data).

Необходимо отдельно рассмотреть регулирование права на забвение, которое подразумевает уничтожение данных пользователей, так как вопрос о хранении персональных данных становится все более актуальным. В соответствии со статьей 17 GDPR, физическое лицо имеет право на незамедлительное удаление персональных данных контроллером, ответственным за обработку данных. Иными словами, данное право позволяет пользователям удалять видеоконтент, фотографии или любую другую информацию о себе, чтобы таким образом она стала недоступной для поисковых систем.

Чтобы воспользоваться правом на забвение и запросить удаление из поисковой системы, необходимо заполнить форму через сайт данной поисковой системы. Процесс запроса на удаление данных в Google требует от заявителя указания страны своего проживания, личной информации, списка подлежащих удалению URL-адресов, краткого описания каждого из них и приложения юридической идентификации [2. – С. 163]. Заявитель получает электронное письмо от Google, подтверждающее его запрос. Если он будет одобрен, персональные данные пользователя будут стерты.

Аналогичная процедура описывается в Федеральном законе № 152: «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. Хранение персональных данных должно осуществляться не дольше, чем этого требуют цели обработки 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».

Также с 1 января 2016 г. вступили в силу поправки к федеральному закону об информации[1]. Согласно данным поправкам, граждане Российской Федерации имеют право обратиться к поисковым системам с запросом об удалении ссылок. Для этого следует так же, как в случае с Google, заполнить форму на сайте соответствующей поисковой системы, перечислив URL страниц, которые заявитель желает исключить из результатов поиска, а также указав причину обращения: распространение информации с нарушением законодательства Российской Федерации, недостоверность либо неактуальность представленных данных. Подобные формы обращения предлагают Mail.ru и «Яндекс». С момента вступления в силу поправок к федеральному закону об информации по состоянию на 25 марта 2016 г. «Яндекс» получил более 3 600 обращений от 1 348 человек, 27% обращений были удовлетворены полностью, 9% – частично, на 73% обращений «Яндекс» ответил отказом [2. – С. 163].

Анализируя деятельность контроллеров (согласно GDPR) и юридических лиц, осуществляющих сбор персональных данных (согласно Федеральному закону № 152), можно выделить следующие общие обязанности:

– принимать технические и организационные меры;

– документировать деятельность по обработке данных;

– оценивать риски;

– обеспечивать безопасность данных.

Существенным преимуществом GDPR перед Федеральным законом № 152 является закрепленная на законодательном уровне обязанность извещать регулятора и граждан о проблемах с данными [12].

Невыполнение правил GDPR ведет к наложению крупных штрафов вплоть до 20 млн евро или до 4% выручки. Максимальный штраф за нарушение закона «О персональных данных» составляет 75 000 рублей [4].

Регулярное систематическое наблюдение является приоритетным механизмом защиты персональных данных, согласно GDPR, и включает:

– мониторинг через умные устройства;

– трекинг местонахождения;

– видеомониторинг;

– программы лояльности;

– поведенческую рекламу;

– создание профилей и скоринг для оценки рисков.

GDPR выделяет специальные категории персональных данных, которые требуют особых правил обработки и защиты:

– медицинские данные;

– данные о сексуальной ориентации;

– генетические данные;

– данные о политических и религиозных взглядах;

– данные об этническом происхождение;

– данные о членстве в профсоюзе;

– биометрические данные для идентификации;

– данные о правонарушениях;

– данные об уголовных приговорах [9. – С. 28].

Рассмотрим ряд примеров применимости требований GDPR к организациям, работающим в разных сферах экономики.

1. *Торговая площадка в интернете*. На специальном веб-сайте представлены товары продавцов из Китая покупателям из стран ЕС, России и США. На сайте представлена возможность совершать покупки, включая их оплату и доставку, а также предъявлять претензии в техническую поддержку. При этом центр обработки данных может находиться либо в России, либо в ЕС, а разработчики сайта – в России. Деятельность ведется от имени нескольких юридических лиц [9. – С. 37].

В данном случае требования GDPR применимы ввиду того, что в процессе заказа товаров происходят сбор и обработка персональных данных граждан ЕС, таргетирование рекламы и индивидуальных предложений для них, а также обработка платежей и претензий.

2. *Интернет-магазин программного обеспечения*. Данный интернет-магазин является технологической платформой для организации взаимодействия покупателей и производителей программного обеспечения. Деятельность осуществляется по всему миру от имени нескольких юридических лиц. Следует отметить, что есть адресные коммуникации для лиц, находящихся в странах ЕС, а разработчики сайта и центра обра-

[1] Федеральный закон от 13 июля 2015 г. № 264-ФЗ «О внесении изменений в Федеральный закон "Об информации, информационных технологиях и о защите информации» и статьи 29 и 402 Гражданского процессуального кодекса Российской Федерации"».

ботки данных находятся на территории Российской Федерации [9. – С. 38].

Можно сделать вывод, что требования GDPR применимы. Это объясняется тем, что осуществляется сбор и обработка данных граждан ЕС и передача их производителям программного обеспечения.

3. *Российская часть глобальной розничной торговой сети*. Штаб-квартира сети находится на территории ЕС. Продажа товаров осуществляется через сеть магазинов организации на территории России. Предусматривается информационная рассылка через СМС-сообщения и сообщения по электронной почте. Целевой аудиторией являются лица, находящиеся на территории России.

В связи с тем, что наблюдается полное отсутствие ориентации фирмы на граждан ЕС или лиц, находящихся на его территории, требования GDPR не применимы [9. – С. 39].

4. *Логистическая компания, осуществляющая перевозки грузов между Европейским союзом и Россией*. Компания имеет собственный парк автомобилей, а также штат сотрудников, состоящий из водителей и экспедиторов – граждан ЕС и СНГ.

Требования GDPR применимы, так как предусмотрены сбор и обработка персональных данных водителей и экспедиторов, находящихся на территории ЕС.

5. *Разработчики и издатели компьютерных игр*. На технологической платформе представлены различные компьютерные игры и аксессуары к ним с целью продажи, включая оплату, перевод платежей производителям, доставку. Заказ можно сделать из любой точки мира, к тому же центры обработки данных расположены в разных юрисдикциях. Деятельность осуществляется от имени нескольких юридических лиц, и есть адресные коммуникации для лиц, находящихся на территории ЕС [9. – С. 41].

Требования GDPR применимы, потому что предусмотрена работа с персональными данными граждан ЕС.

Требования GDPR применимы и к таким организациям, как пассажирско-транспортная компания, осуществляющая перевозку пассажиров Россия – ЕС, ЕС – Россия; аренда автомобилей с возможностью выезда на арендованном автомобиле в ЕС; туристическая компания, организующая туры по Российской Федерации для клиентов из ЕС. Все эти компании объединяет тот факт, что для их деятельности необходимы сбор и обработка личных данных клиентов из ЕС [9. – С. 44].

Таким образом, многим фирмам, осуществляющим свою деятельность на территории России, но ориентированным на рынок ЕС, необходимо внедрить в организацию своей деятельности принципы GDPR.

Итак, можно выделить пять этапов внедрения GDPR.

Во-первых, необходимо проанализировать существующие бизнес-процессы организации и потоки данных. Выявить, обрабатываются ли персональные данные лиц, находящихся в ЕС, а также проанализировать применяемые для обработки персональных данных технологии. На основе этого нужно определить область применения GDPR.

Во-вторых, нужно выявить, какие процессы и системы требуют изменения для соответствия требованиям GDPR; определить потенциальные риски, связанные с GDPR, определить их приоритетность; разработать стратегию по приведению деятельности компании в соответствие с требованиями GDPR.

В-третьих, следует сформировать детальный план действий, необходимых для приведения процессов организации в соответствие с требованиями GDPR, а также определить необходимые ресурсы для проведения трансформации, ответственных за трансформацию лиц, и в дополнение к этому определить приоритетность выполнения задач, согласовать сроки выполнения со всеми заинтересованными сторонами.

В-четвертых, нужно спроектировать и реализовать внедрение организационных мер, необходимых для соответствия GDPR и обеспечить вовлеченность всех заинтересованных сторон в трансформацию процессов обработки и хранения персональных данных.

В-пятых, любая система требует регулярных проверок и обслуживания. В виду этого необходимо постоянно проводить анализ соответствия деятельности информационной системы организации требованиям GDPR.

Некоторые интернет-компании уже следуют требованиям GDPR. Например, популярная социальная сеть «ВКонтакте» хранит большую базу данных о своих пользователях. Так, отслеживается изменение имени пользователя, управление группами, все файлы и переписки, даже те, которые были удалены, все опубликованные записи и

комментарии за много лет [3]. В соответствии с Правилами защиты информации о пользователях сайта VK.com, приоритетной задачей правил является обеспечение надлежащей защиты информации о пользователях, в том числе их персональных данных, от несанкционированного доступа и разглашения [5].

Тем не менее как в российской, так и в зарубежной практике компании столкнулись с трудностями после принятия Общего регламента по защите данных. Так, первое судебное решение было принято в Германии. Сторонами разбирательства были интернет-корпорация по присвоению имен и номеров (ICANN) и регистратор EPAG Domainservices GmbH. ICANN стремилась обязать EPAG соблюдать «соглашение об аккредитации регистраторов», которое требует от регистраторов собирать административную и техническую контактную информацию для регистрации нового доменного имени. Суд постановил, что ICANN не может достоверно доказать, что сбор административной и технической контактной информации необходим в соответствии со статьей 5 GDPR, которая устанавливает, что личные данные могут собираться только для определенных, явных и законных целей и должны быть адекватными, релевантными и ограниченными тем, что необходимо в связи с целью. Поэтому EPAG не обязана собирать такие данные [11].

Другим спорным моментом является так называемая уличная фотография. В соответствии с GDPR, к персональным данным относится внешность человека, в связи с чем нельзя распространять фотографии людей, не получив при этом их согласия. Исключение сделано для публикации в общественных интересах, сбора информации для архивов или научных исследований, а также для полиции, если, например, речь идет о фото преступника (статья 89 GDPR) [10].

При этом съемка может осуществляться свободно. К примеру, если фотограф запечатлел людей на оживленной площади без их согласия, то, чтобы не нарушить закон, он может представить это фото публике, размазав изображения лиц, полностью уничтожив эстетичность.

Санкции, предусмотренные за нарушение регламента, направлены в первую очередь на крупные компании, хранящие персональные данные пользователей, например, Facebook или Google. Так, появление GDPR было спровоцировано серией скандалов с утечками информации из социальных сетей. Один из таких примеров – консалтинговая компания Cambridge Analytica, которая собрала персональные данные 50 млн пользователей Facebook, чтобы затем продавать им таргетированную политическую рекламу [13]. За такие действия теперь предусмотрены крупные штрафы.

В то же время для частных лиц финансовые санкции за нарушение новых требований в регламенте не прописаны. Однако в комментариях к регламенту оговаривается, что сумма штрафов устанавливается с учетом доходов человека и что финансовое взыскание можно заменить на предупреждение, если нарушение совершено впервые и является незначительным [8].

Таким образом, несмотря на то, что принятие GDPR является важным шагом в регулировании информационных потоков, судебная практика находится на стадии формирования. Многие организации ждут возникновения правоприменительной практики для правовой определенности в работе с данными.

Список литературы

1. Анализ возможных последствий и влияния Регламента General Data Protection Regulation (GDPR) Европейского союза на бизнес российских операторов персональных данных, предоставляющих услуги через интернет для лиц в странах ЕС в контексте действующего и вступающего в силу регулирования в Российской Федерации. – URL: https://internetinstitute.ru/wp-content/uploads/2017/10/GDPR.pdf (дата обращения: 12.01.2019).

2. *Леденцова И. А.* Право на забвение: можно ли затеряться в виртуальной толпе? // Электронное приложение к Российскому юридическому журналу. – 2017. – № 3. – С. 161–164.

3. Какие данные «ВКонтакте» выдает пользователям из Евросоюза по GDPR. – URL: https://tjournal.ru/law/75265-kakie-dannye-vkontakte-vydaet-polzovatelyam-iz-evrosoyuza-po-gdpr (дата обращения: 17.01.2019).

4. Ответственность за нарушение закона о персональных данных. – URL: http://www.garant.ru/actual/persona/otvetstvennost/ (дата обращения: 12.01.2019).

5. Правила защиты информации о пользователях сайта VK.com. – URL: https://vk.com/privacy (дата обращения: 17.01.2019).

6. *Стукалов А. С.* Европейская модель регулирования информационных отношений в сети «Интернет» // Проблемы экономики и юридической практики. – 2017. – № 1. – С. 129–132.

7. *Удовиченко Ю. Г., Ногаева В. У*. General Data Protection Regulation // Актуальные проблемы российского права. – 2018. – № 8 (93). – С. 221–224.

8. Data Breach Statistics. – URL: http://breachlevelindex.com (дата обращения: 12.01.2019).

9. GDPR: практика реализации требований. – URL: http://www.aig.ru/content/dam/aig/emea/russia/documents/reports/gdpr_pwc.pdf (дата обращения: 12.01.2019).

10. General Data Protection Regulation. – URL: https://gdpr-info.eu/ (дата обращения: 17.01.2019).

11. Germany: First Court Decision on GDPR. – URL: https://blogs. dlapiper.com/privacymatters/germany-first-court-decision-on-gdpr/ (дата обращения: 17.01.2019).

12. 2018 Reform of EU Data Protection Rules. – URL: https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en (дата обращения: 17.01.2019).

13. *Cadwalladr C*., *Graham-Harrison E*. Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach. – URL: http://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election (дата обращения: 17.01.2019).