

REFERENCES

1. Dolgova A. I. Criminological assessments of organized crime and corruption, legal battles and national security. M., 2011. 665 p. (In Russ.).
2. Kudryavtsev V. N. Causality and determinism in criminology. Vladivostok, 1983. Pp. 4–10. (In Russ.).
3. Eminov V. E. The causes of crime in Russia: criminological and socio-psychological analysis. M., 2011. 128 p. (In Russ.).
4. Antonyan Yu. M. Criminology. M., 2012. 388 p. (In Russ.).
5. Shestakov D. A. Criminology: new approaches to crime and criminology. SPb., 2006. 561 p. (In Russ.).
6. Koroleva M. V. Corruption: the state of counteraction and the direction of optimization of the struggle // The state of counteracting corruption and the direction of improving the fight against it. Materials of the All-Russian scientific-practical conference. M., 2015. Pp. 71–78. (In Russ.).
7. Makarov V. V. Self-determination of crime. M., 2015. 144 p. (In Russ.).
8. Brief philosophical encyclopedia. M., 1994. 575 p.
9. Gordeeva T. O. Self-determination theory: present and future. Part 1. Problems of the development of the theory // Psychological studies: electron. scientific journals 2010. No. 4 (12). (In Russ.). URL: <http://psystudy.ru/num/2010n4-12/343-gordeeva12>.
10. Dolgova A. I., Vanyushkin S. V., Evlanova O. A., Ilyin O. S., Koroleva M. V., Serebryakova V. A., Yutskova E. M. Crime in Russia: statistics and realities // Crime, statistics, law. M., 1997. Pp. 4–10. (In Russ.).
11. Koroleva M. V. Criminological evaluation of modern recurrent crime in Russia // Russian criminological view. 2015. No. 1. Pp. 125–130. (In Russ.).
12. Bochkareva E. V. Organized crime as a form of crime self-determination // Spirit-time. 2018. No. 12. Pp. 77–82. (In Russ.).
13. Smirnov A. M. Mob law in Russia. M., 2013. 384 p. (In Russ.).
14. Starkov O. V. Criminal subculture: special course. M., 2010. 240 p. (In Russ.).
15. Bochkareva E. V. Legal anomie and criminalization of modern Russian society // Bulletin of CSU. Series “Law”. 2018. No. 3. Pp. 70–74. (In Russ.).

Как цитировать статью: Бочкарева Е. В. Самодетерминация преступности: понятие и формы // Бизнес. Образование. Право. 2019. № 1 (46). С. 379–383. DOI: 10.25683/VOLBI.2019.46.149.

For citation: Bochkareva E. V. Self-determination of crime: concept and forms // Business. Education. Law. 2019. No. 1 (46). Pp. 379–383. DOI: 10.25683/VOLBI.2019.46.149.

УДК 341.1/8
ББК 67.91

DOI: 10.25683/VOLBI.2019.46.150

Vlasov Roman Borisovich,

Post-graduate student of the department of the constitutional and international law, the All-Russian state university of justice (RAJ of the RF Ministry of Justice), Moscow,
e-mail: vlasoff.vel@yandex.ru

Власов Роман Борисович,

соискатель кафедры конституционного и международного права, Всероссийский государственный университет юстиции (РПА Минюста России), г. Москва
e-mail: vlasoff.vel@yandex.ru

**ПРИМЕНЕНИЕ ОБЩЕГО РЕГЛАМЕНТА ЕВРОПЕЙСКОГО СОЮЗА
ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ К РОССИЙСКИМ КОМПАНИЯМ:
ПРОБЛЕМЫ И СПОСОБЫ ИХ РЕШЕНИЯ**

**EUROPEAN UNION GENERAL DATA PROTECTION REGULATION
APPLICATION TO THE RUSSIAN COMPANIES:
PROBLEMS AND METHODS OF SOLUTION**

12.00.10 – Международное право; европейское право

12.00.10 – International law; European law

Настоящая статья посвящена вопросу применения нового Общего регламента Европейского союза по защите персональных данных к российским компаниям. На основе анализа критериев применимости Регламента к российским компаниям автор приходит к выводу, что не все критерии сформулированы ясно и однозначно, в связи с чем отечественные компании могут столкнуться с неопределенностями при их толковании. По результатам исследования автор пришел к заключению, что российская дочерняя компания

материнской компании из Европейского союза подпадает под действие Регламента, поскольку между деятельностью материнской компании и обработкой персональных данных в дочерней компании имеется неразрывная связь. Кроме того, автор обосновывает позицию, согласно которой для применения к российской компании Регламента при осуществлении его мониторинга поведения субъекта персональных данных такой мониторинг должен быть основной целью деятельности компании, а не частью ее продукта или услуги.

The present article examines application of new European Union General Data Protection Regulation to the Russian companies. Based on the analysis of the criteria of applicability of the GDPR to the Russian companies, the author concludes that not all criteria are formulated clearly and unequivocally, and therefore domestic companies may encounter uncertainties in their interpretation. According to the results of the study, the author came to the conclusion that the Russian subsidiary of the parent company from the European Union falls within the scope of the GDPR, since the subsidiary has an inextricable link between the activities of the parent company and the processing of personal data. In addition, the author substantiates the position that, in order for applicability of GDPR to the Russian company when it monitors the behavior of the subject of personal data, such monitoring should be the main goal of the company, but not the part of its product or service.

Ключевые слова: персональные данные, GDPR, обязательные корпоративные правила, информационное право, Европейский союз.

Keywords: personal data; GDPR; binding corporate rules; informational law; European Union.

Введение

Совсем недавно в Европейском союзе появились новые правила обработки и защиты персональных данных, которые были закреплены в новом Регламенте — GDPR. GDPR имеет экстерриториальный характер, и его действие распространяется на компании, которые осуществляют деятельность и за пределами Европейского союза. Соответственно, российские компании при определенных условиях также могут подпадать под действие GDPR, а значит, должны выполнять его требования. В GDPR сформулированы критерии, которые устанавливают применимость документа к компаниям, расположенным за пределами ЕС, однако критерии применимости GDPR сформулированы недостаточно четко, что влечет для российских компаний неопределенность и неясность при решении вопроса о том, подпадают ли они под действие GDPR или нет. Это вызывает необходимость дополнительного толкования критериев, установленных GDPR. Этим обусловлена **актуальность** настоящей статьи.

В то время как исследованию вопросов обработки и защиты персональных данных в ЕС посвящен ряд работ российских и зарубежных авторов, отдельные аспекты становятся предметом самостоятельного исследования довольно редко. В российской науке нет самостоятельных исследований, посвященных применимости GDPR к компаниям, осуществляющим свою деятельность на территории Российской Федерации. Этим объясняется **целесообразность** разработки настоящей темы.

Научная новизна исследования подтверждается получением новых научных результатов, состоящих в обосновании выводов, касающихся применения GDPR к российским компаниям.

Теоретическое значение настоящей работы состоит в том, что она является результатом теоретического исследования, которое вносит вклад в научное осмысление практики применения и реализации международно-правового документа российскими организациями из сферы бизнеса. **Практическое значение** результатов исследования обусловлено возможностью их использования

российскими компаниями при осуществлении деятельности, которая тем или иным образом направлена на территорию Европейского союза.

Целью настоящей работы является анализ обстоятельств, при которых российские компании подпадают под действие GDPR. Для достижения этой цели автором были поставлены следующие **задачи**: во-первых, рассмотреть критерии применимости GDPR к компаниям, расположенным за пределами Европейского союза; во-вторых, изучить ситуации, когда при формальной применимости GDPR к деятельности российских компаний выполнять требование GDPR необязательно; и, в-третьих, проанализировать применимость GDPR к российским дочерним компаниям, материнская компания которых расположена в ЕС.

Основная часть

25 мая 2018 г. Европейский союз официально перешел на новые правила обработки и защиты персональных данных. Именно в этот день вступил в силу Общий регламент по защите персональных данных ЕС 2016/679 от 27 апреля 2016 г. (GDPR) (далее – Регламент). Прежде обработка и защита персональных данных в ЕС регулировалась Директивой 95/46/ЕС Европейского парламента и Совета Европейского союза от 24 октября 1995 г. о защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных (далее — Директива 95/46/ЕС). Причиной пересмотра положений Директивы 95/46/ЕС и принятия Регламента послужили, прежде всего, развитие информационных технологий, появление новых способов обработки и анализа информации, новые вызовы безопасности личных данных граждан. Как следствие, основные нововведения Регламента по сравнению с Директивой посвящены новым правам субъектов персональных данных в связи с появлением новых способов обработки этих данных. Кроме того, действие Регламента теперь носит экстерриториальный характер. Это означает, что его требования распространяются на операции по обработке персональных данных как на территории Европейского союза, так и за его пределами. Соответственно, в сферу действия Регламента подпадают и компании, осуществляющие свою деятельность на территории ЕС, и компании, осуществляющие свою деятельность в странах — не членах Европейского союза при наличии определенных условий. В этой связи перед многими российскими компаниями встал вопрос о применимости к ним требований Регламента.

Критерии применимости положений Регламента установлены в ст. 3. Так, ч. 1 ст. 3 устанавливает, что Регламент применяется к лицам, образованным вне территории ЕС, если осуществляется обработка персональных данных в контексте деятельности подразделения контролера или обработчика персональных данных в ЕС. При этом не имеет значения, осуществляется ли такая обработка на территории или вне территории ЕС. В свою очередь, ч. 2 ст. 3 предусматривает, что Регламент применяется к лицам, образованным вне территории ЕС, если осуществляется обработка персональных данных находящихся на территории ЕС субъектов персональных данных контролером или обработчиком, не имеющим подразделения в ЕС, и при этом такая обработка связана с: 1) предложением товаров или услуг находящимся на территории ЕС субъектам данных или 2) мониторингом поведения

находящихся на территории ЕС субъектов персональных данных при условии, что такое поведение имеет место на территории ЕС [1].

Таким образом, российские компании будут подпадать под действие Регламента в следующих случаях:

1) обработка персональных данных осуществляется в контексте деятельности подразделения контролера или обработчика персональных данных в ЕС;

2) если обработка персональных данных связана с предложением товаров и услуг находящимся на территории ЕС субъектам персональных данных;

3) если обработка персональных данных связана с мониторингом поведения находящихся на территории ЕС субъектов персональных данных при условии, что такое поведение имеет место на территории ЕС.

При толковании первого пункта возникает вопрос о том, что является подразделением контролера или обработчика персональных данных. Очевидно, что когда российская компания является материнской по отношению к европейской дочерней структуре либо когда российская компания имеет филиал или представительство в Европейском союзе, то она подпадает под действие Регламента, поскольку все находящиеся в Европейском союзе юридические лица являются субъектами Регламента независимо от их организационно-правовой формы, а значит, являются подразделениями по смыслу Регламента.

Однако применительно к этому положению Регламента противоположная ситуация, когда материнская компания, находящаяся в ЕС, имеет дочернюю компанию в России, не выглядит столь очевидной. Возникает резонный вопрос: должна ли российская дочерняя компания соблюдать требования Регламента автоматически, поскольку она является подразделением по смыслу Регламента, или для этого необходимо требование материнской компании о соблюдении Регламента?

Представляется, что при определении понятия «подразделение», предусмотренного ч. 1 ст. 3 Регламента, в основу должен быть положен критерий тесной связи между таким подразделением и непосредственно обработкой персональных данных. То есть если обработка персональных данных происходит в российской дочерней компании, то европейская материнская компания в обработку персональных данных фактически не вовлечена. Но поскольку между материнской и дочерней компаниями существует неразрывная связь по определению, то в качестве частного случая проявления такой связи следует рассматривать связь между деятельностью материнской компании в ЕС и обработкой персональных данных, которая осуществляется в ее дочерней структуре в России. Исходя из этого, российская дочка европейской материнской компании подпадает под действие Регламента [2, с. 22].

Такой вывод может быть поддержан толкованием и применением ранее действовавшей Директивы 95/46/ЕС, которая также использовала понятие «подразделение» [3]. Так, Рабочая группа ст. 29 по применению Директивы 95/46/ЕС в одном из своих разъяснений высказала позицию о том, что понятие «подразделение» должно толковаться широко, и законодательство Европейского Союза в части защиты персональных данных может применяться даже в случае, когда подразделение в Европейском Союзе в обработку персональных данных напрямую не вовлечено, но между деятельностью такого подразделения и обработкой персональных данных существует неразрывная связь.

Таким образом, можно сделать вывод о том, что российская дочерняя компания материнской европейской компании подпадает под действие Регламента и должна соблюдать его требования. Но в любом случае практика применения Регламента по этому вопросу появится в ближайшее время и даст однозначный ответ.

Тем временем автор предлагает также обратить внимание на предусмотренный Регламентом механизм, который позволяет применять Регламент к российским дочерним компаниям материнских компаний из Европейского Союза по требованию последних, избежав неопределенности (до появления однозначной практики применения Регламента) в вопросе распространения на российские дочерние компании требований Регламента. Этим механизмом являются обязательные корпоративные правила (Binding corporate rules), закрепленные в ст. 47 Регламента. Фактически обязательные корпоративные правила — это предусмотренная Регламентом возможность для европейских компаний, ведущих совместный бизнес с компаниями, расположенными за пределами ЕС, устанавливать единые правила обработки и защиты персональных данных для всех участников группы. В статье 47 Регламента закреплены требования к содержанию обязательных корпоративных правил. Так, они должны определять структуру группы компаний, категории персональных данных, типы субъектов персональных данных и их права, принципы защиты персональных данных, порядок рассмотрения жалоб субъектов персональных данных, а также порядок проведения аудита и отчетности перед надзорными органами. А для того чтобы обязательные корпоративные правила были обязательными для всех участников группы компаний, они должны быть разработаны для целей конкретной группы компаний, утверждены надзорным органом в области защиты персональных данных той страны, где имеет свое местонахождение материнская компания, и подписаны всеми участниками группы компаний [1].

Таким образом, российская дочерняя компания материнской компании из ЕС при подписании обязательных корпоративных правил, установленных материнской компанией, становится обязанной соблюдать Регламент. Представляется, что для материнской компании огромный плюс такого механизма заключается в возможности соблюдения требований Регламента при взаимодействии со своими неевропейскими структурами в части трансграничной передачи персональных данных своих сотрудников, а также клиентов и потребителей, что является неотъемлемой частью информационного взаимодействия внутри любой группы компаний [4, с. 7].

Кроме того, положения Регламента являются наиболее передовыми во всем мире, и их соблюдение почти наверняка позволит соответствовать требованиям российского законодательства о персональных данных [5, с. 161].

К тому же соблюдение Регламента является большим репутационным преимуществом, так как свидетельствует о высоких стандартах защиты и обработки персональных данных в компании.

При анализе возможности применения второго пункта (предложение товаров или услуг находящимся на территории ЕС субъектам данных) к российским компаниям необходимо отметить, что одного наличия доступа у субъекта персональных данных из ЕС к вебсайту российской компании, на котором предлагаются товары или услуги,

недостаточно, поскольку в таком случае сфера применения Регламента носила бы, по существу, всемирный характер и делала бы практически невозможным контроль за исполнением вебсайтом требований Регламента. Аналогичного мнения придерживаются и зарубежные авторы при анализе применимости GDPR к компаниям, расположенным за пределами Европейского союза [6, с. 24].

Представляется, что для распространения Регламента на российские компании, предлагающие товары или услуги европейцам, обязательным условием должно являться наличие явной цели российской компании сделать субъектов персональных данных из Европейского союза своими клиентами. Об этом свидетельствует также европейский судебный опыт толкования положений о направленной деятельности [7].

Примечательно, что критерий направленной деятельности как условие распространения законодательства о персональных данных на иностранное лицо, не имеющее присутствия на территории страны — члена Европейского союза, пришел на смену критерию местонахождения оборудования, расположенного на территории Европейского союза, содержащемуся в ст. 4 (1) Директивы 1995 г. [3]. Но критерий местонахождения оборудования подвергался частой критике, поскольку много споров вызывало само понятие «оборудование», и критерий создавал условия для обхода обременительных требований Европейского союза посредством искусственного подчинения правоотношения правопорядку другого государства, на территории которого находятся соответствующие мощности [8].

Стоит отметить, что при распространении российского закона о персональных данных на иностранных лиц также используется критерий направленности деятельности. Так, Минкомсвязи выделяет следующие критерии: 1) использование географического доменного имени, связанного с РФ; 2) наличие русскоязычной версии интернет-ресурса; 3) возможность заключения и исполнения договора с российским резидентом; 4) возможность осуществления расчетов в российских рублях; 5) использование контекстной или баннерной рекламы на русском языке [9].

Учитывая вышеизложенное, автор полагает, что о наличии явной цели российской компании сделать субъектов персональных данных из ЕС своими клиентами могут свидетельствовать следующие факторы:

1. Размещение сайта под доменным именем в зоне одной из стран Европейского союза (например, .de, .it, .pl). Этот критерий основан на презумпции, согласно которой регистрация и фактическое использование доменного имени в указанных зонах являются проявлением намерения владельца интернет-ресурса осуществлять свою деятельность в отношении стран Европейского союза, что обусловлено географической привязкой доменов к территории стран ЕС.

2. Предложение товаров или услуг на вебсайте на одном из языков страны Европейского союза. Использование языка одной из стран Европейского союза на интернет-ресурсе является сильным аргументом в пользу присутствия направленной деятельности такого сайта на территорию ЕС безотносительно к его доменному имени. При этом во внимание должна приниматься именно целенаправленная локализация интернет-сайта, осуществленная самим владельцем сайта или иным привлеченным им лицом, применение систем автоматического перевода не должно приниматься во внимание [10, с. 34].

3. Прием валюты страны Европейского Союза для оплаты товаров или услуг.

4. Возможность размещения заказов на языке одной из стран Европейского Союза.

5. Возможность доставки товара или оказания услуги по адресу в одной из стран Европейского Союза.

При толковании третьего пункта (если обработка персональных данных связана с мониторингом поведения находящихся на территории ЕС субъектов персональных данных при условии, что такое поведение имеет место на территории Европейского Союза) также возникает неоднозначная ситуация.

Мониторинг поведения субъекта персональных данных имеет место, когда компания отслеживает поведение и действия физических лиц в сети Интернет и использует полученную информацию в целях составления профайла лица для принятия решений в отношении него или предсказания его личных предпочтений или привычек [11].

Фактически это положение Регламента означает, что любой российский банк становится субъектом Регламента, как только его клиент выезжает на территорию ЕС. Это связано с тем, что неотъемлемой частью банковских услуг является мониторинг местонахождения клиента. Если клиент снимает денежные средства в банкомате страны ЕС, то в реестре банковских операций автоматически фиксируется факт снятия наличных средств с указанием местонахождения банкомата. По смыслу Регламента указанные действия свидетельствуют о мониторинге со стороны банка местонахождения клиента. Владелец карты в момент оплаты находится на территории ЕС, и формально сбор данных в этом случае отвечает признакам мониторинга активности, что, соответственно, влечет применение Регламента.

Но, с другой стороны, представляется, что мониторинг поведения субъекта персональных данных в сети Интернет должен быть основной целью деятельности компании, а не частью ее продукта или услуги [4, с. 13]. Ведь если банк не таргетирует европейских клиентов и не использует эти данные для маркетинга или иных целей, помимо соблюдения банковского регулирования и обеспечения безопасности транзакций, иначе говоря, никак не развивает эти данные, то существуют определенные предпосылки говорить, что такой сбор информации не является мониторингом в том смысле, который изначально закладывался при разработке Регламента.

Во многом это объясняется духом Регламента, согласно которому мониторинг поведения субъектов персональных данных в Интернете должен быть целью деятельности компании, основным видом ее деятельности [2]. Кроме того, некоторые зарубежные авторы полагают, что мониторинг должен составлять именно существенную часть деятельности компании [12, с. 37]. В этой связи, по мнению автора, описанная выше ситуация не должна подпадать под это положение Регламента, а российский банк, соответственно, под действие Регламента. Мониторинг поведения субъекта персональных данных в сети Интернет должен быть основной целью деятельности компании, и, соответственно, этот критерий касается различного рода интернет-сервисов, которые осуществляют сбор пользовательских данных в целях их последующего использования для предоставления таргетированной рекламы. Так, приехав в одну из стран ЕС, россиянин использует какие-либо мобильные приложения, через которые

российский владелец приложения, отслеживая геопозицию пользователя, может предлагать ему рекламу находящихся поблизости кафе, ресторанов или достопримечательностей. В этом случае владелец мобильного приложения также будет подпадать под требования Регламента, хоть и находится на территории России.

В качестве примеров деятельности российской компании, подпадающей под действие Регламента, можно привести следующие.

Российская логистическая компания занимается автомобильными грузоперевозками между Россией и странами Европейского Союза. Компания имеет собственный парк автомобилей, а водители и экспедиторы, состоящие в штате компании, являются гражданами России. При этом компания осуществляет мониторинг движения транспортных средств, а также мониторинг времени, проведенного водителями за рулем своего автомобиля. Соответственно, компания осуществляет сбор и обработку персональных данных водителей и экспедиторов во время их нахождения на территории ЕС. Учитывая, что осуществляется обработка данных лиц, находящихся на территории ЕС, российская логистическая компания подпадает под действие Регламента.

Аналогичный вывод можно сделать и по отношению к российскому оператору аренды автомобилей с возможностью выезда на арендованном автомобиле в страны Европейского союза, так как имеет место мониторинг движения автомобиля и отслеживание текущего местоположения. Учитывая, что в данной ситуации имеет место сбор и обработка персональных данных арендаторов автомобилей, находящихся на территории ЕС (в случае их выезда), а также сбор и обработка данных об административных правонарушениях лиц, находящихся на территории ЕС (в случае их выезда), российская компания подпадает под действие Регламента.

Аналогичным образом требования Регламента применимы и к российским туристическим компаниям, которые занимаются организацией туров в России и за рубежом для клиентов из стран ЕС. Бронируя гостиницы, а также авиа- и железнодорожные билеты для клиентов из Европейского союза, компания обрабатывает персональные данные лиц, находящихся на территории Европейского союза, и, соответственно, должна соблюдать требования Регламента.

Заключение и выводы

Таким образом, российские компании подпадают под действие Регламента в следующих случаях.

Во-первых, когда российская компания является материнской по отношению к европейской дочерней струк-

туре либо когда российская компания имеет филиал или представительство в Европейском союзе. Автор также приходит к выводу, что российская дочерняя компания материнской компании из Европейского союза подпадает под действие Регламента, поскольку между ними имеется неразрывная связь, частным случаем проявления которой является связь между деятельностью материнской компании в Европейском союзе и обработкой персональных данных, которая осуществляется в ее дочерней структуре в России.

Во-вторых, когда российская компания предлагает товары и услуги находящимся на территории ЕС субъектам персональных данных. При этом обязательным условием является наличие явной цели российской компании сделать субъектов персональных данных из ЕС своими клиентами. О явной цели могут свидетельствовать следующие факторы: 1) размещение сайта под доменным именем в зоне одной из стран Европейского союза (например, .de, .it, .pl); 2) предложение товаров или услуг на вебсайте на одном из языков страны Европейского союза; 3) прием валюты страны Европейского союза для оплаты товаров или услуг; 4) возможность размещения заказов на языке одной из стран Европейского союза; 5) возможность доставки товара или оказания услуги по адресу в одной из стран Европейского союза.

В-третьих, когда российская компания осуществляет мониторинг поведения субъекта персональных данных. Мониторинг имеет место, когда компания отслеживает поведение и действия физических лиц в сети Интернет и использует полученную информацию в целях составления профайла лица для принятия решений в отношении него или предсказания его личных предпочтений или привычек. При этом дискуссионным является вопрос о таком мониторинге, который является лишь частью продукта или услуги компании. Автор делает вывод, что мониторинг поведения субъекта персональных данных в сети Интернет должен быть основной целью деятельности компании, а не частью ее продукта или услуги, поскольку если компания не использует полученные при мониторинге данные для маркетинга или иных целей, помимо сопровождающих продукт или услугу, иначе говоря, никак не развивает эти данные, то такой сбор информации не является мониторингом в том смысле, который изначально закладывался при разработке Регламента.

Однако в любом случае окончательные ответы на спорные вопросы, связанные с Регламентом и российскими компаниями, даст лишь практика применения этого международного акта.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. 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) // European Union official website. URL: http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf
2. Ковалева Н. Российские дочки европейских компаний: нужно ли следовать Общему Регламенту по защите персональных данных (GDPR) // Legal Insight. 2018. № 5. С. 21–25.
3. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data // European Union official website. URL: <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&qid=1512661273236&from=EN>
4. Коморовский П. Корпоративное управление и новый GDPR (Общий Регламент по защите персональных данных). GRIN Verlag. 2018. 30 с.

5. Савельев А. И. Научно-практический постатейный комментарий к Федеральному закону «О персональных данных». М. : Статут, 2017. 320 с.
6. Paul Voigt, Axel von dem Bussche. The EU General Data Protection Regulation (GDPR): A Practical Guide // Springer International Publishing. 2017. 383 p.
7. Joined cases: Peter Pammer v. Reederei Karl GmbH & Co. KG (C-585/08) and Hotel Alpenhof GesmbH v. Oliver Heller (C-144/09), 7 December 2010. URL: <http://curia.europa.eu/juris/liste.jsf?language=en&num=C-585/08>
8. Opinion 8/2010 On Applicable Law. Article 29 Data Protection Working Party. 16 December 2010. URL: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp179_en.pdf
9. Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации: официальный сайт. URL: <https://digital.gov.ru/ru/personaldata/>.
10. Calder Alan. EU General Data Protection Regulation (GDPR) an Implementation and Compliance Guide // IT Governance Publishing. 2016. 400 p.
11. Дмитриев А. Соответствие GDPR — это далеко не вопрос настройки локальных актов и стандартных документов, как иногда приходится слышать // ЭЖ-Юрист. 2018. № 36. <https://www.eg-online.ru/article/380104/>
12. Punit Bhatia. Be Ready for GDPR: Let Us Check Your Readiness for General Data Protection Regulation (GDPR) // Independently Published. 2017. 186 p.

REFERENCES

1. 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). European Union official website. URL: http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf
2. Kovaleva N. Russian subsidiaries of European companies: should the General Regulations on protection of the personal data (GDPR) be followed // Legal Insight. 2018. No. 5. Pp. 21–25. (In Russ.).
3. Directive 95/46/EC of the European Parliament and the Council dated 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data // European Union official website. URL: <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&qid=1512661273236&from=EN>
4. Komorowsky R.. Corporate Governance and the New GDPR (General Data Protection Regulation). GRIN Verlag. 2018. 30 p. (In Russ.).
5. Savelyev A. I. Scientific and practical article-by-article commentary to the Federal Law “On Personal Data”. М. : Statut, 2017. 320 p. (In Russ.).
6. Paul Voigt, Axel von dem Bussche. The EU General Data Protection Regulation (GDPR): A Practical Guide // Springer International Publishing. 2017. 383 p.
7. Joined cases: Peter Pammer v. Reederei Karl GmbH & Co. KG (C-585/08) and Hotel Alpenhof GesmbH v. Oliver Heller (C-144/09), 7 December 2010. URL: <http://curia.europa.eu/juris/liste.jsf?language=en&num=C-585/08>
8. Opinion 8/2010 On Applicable Law. Article 29 Data Protection Working Party. 16 December 2010. URL: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp179_en.pdf
9. Ministry of Digital Development, Communications and Mass Communications of the Russian Federation official website. (In Russ.). URL: <https://digital.gov.ru/ru/personaldata/>
10. Calder Alan. EU General Data Protection Regulation (GDPR) an Implementation and Compliance Guide // IT Governance Publishing. 2016. 400 p.
11. Dmitriev A. Compliance with the GDPR is far from a matter of setting up the local acts and standard documents as we sometimes hear // EZh-Yurist. 2018. No. 36. (In Russ.). URL: <https://www.eg-online.ru/article/380104/>
12. Punit Bhatia. Be Ready for GDPR: Let Us Check Your Readiness for General Data Protection Regulation (GDPR) // Independently Published. 2017. 186 p.

Как цитировать статью: Власов Р. Б. Применение Общего регламента Европейского союза по защите персональных данных к российским компаниям: проблемы и способы их решения // Бизнес. Образование. Право. 2019. № 1 (46). С. 383–388. DOI: 10.25683/VOLBI.2019.46.150.

For citation: Vlasov R. B. European Union General Data Protection Regulation application to the Russian companies: problems and methods of solution // Business. Education. Law. 2019. No. 1 (46). Pp. 383–388. DOI: 10.25683/VOLBI.2019.46.150.