**УДК** 341.17
**DOI:** 10.19073/2306-1340-2019-16-1-29-35

# ПРИНЦИПЫ ОБЩЕГО РЕГЛАМЕНТА ЕВРОПЕЙСКОГО СОЮЗА О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ (GDPR): ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ ИМПЛЕМЕНТАЦИИ

**ЧУРИЛОВ Алексей Юрьевич***
✉ Lefikantor@yandex.ru
*Пр. Ленина, 36, Томск, 634050, Россия*

***Аннотация.*** *В работе рассмотрены фундаментальные принципы обработки персональных данных, закрепленные в Регламенте № 2016/679 ЕС: законность, справедливость и прозрачность; целевое ограничение; минимизация данных; точность; ограничение хранения; целостность и конфиденциальность; ответственность (подотчетность). Необходимость изучения и имплементации требований, закрепленных в регламенте, связана с экстерриториальностью его действия и потенциальной возможностью распространения его действия на российские компании, оказывающие услуги и продающие товары в странах Европейского союза. По каждому принципу автор дает комментарии относительно сложностей имплементации и рекомендации по применению, а также делает некоторые критические замечания. Освещается раскрытие каждого из принципов в иных статьях Регламента, а также демонстрируется взаимодействие этих принципов друг с другом.*

***Ключевые слова:*** *персональные данные, Европейский союз, принципы, обработка персональных данных, правовое регулирование.*

# Principles of the EU General Regulations for the Protection of Personal Data (GDPR): Problems and Perspectives for Implementation

**Churilov Aleksei Yu.****
✉ Lefikantor@yandex.ru
*36 Lenina pr., Tomsk, 634050, Russia*

***Abstract.*** *The paper discusses the fundamental principles of personal data processing enshrined in EU Regulation No. 2016/679: legality, fairness, and transparency; purpose limitation; data minimization; accuracy; storage limitation; integrity and confidentiality; responsibility (accountability). The need to study and implement the requirements outlined in the regulations is related to the extraterritorial nature of its operation and the potential possibility of extending its operation to Russian companies providing services and selling goods in the European Union countries. The Author gives comments regarding each principle on the difficulties of implementation and recommendations on their application, as well as some critical comments. The Author covers the disclosure of each of the principles in other articles of the Regulations and demonstrates the interaction of these principles with each other.*

***Keywords:*** *personal data, European Union, principles, personal data processing, legal regulation.*

25 мая 2018 г. в силу вступил Регламент № 2016/679 Европейского парламента и Совета Европейского союза «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС»[1] (далее – Регламент, GDPR). Сбор и обработка данных, подпадающие под регулирование Регламента, должны

* Ассистент кафедры гражданского права Национального исследовательского Томского государственного университета.

** Assistant of the Department of Civil Law at National Research Tomsk State University.

[1] *О защите* физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС (Общий Регламент о защите персональных данных) : регламент № 2016/679 Европ. парламента и Совета Европ. союза (принят в г. Брюсселе 27 апр. 2016 г.). Доступ из СПС «КонсультантПлюс».

быть приведены в соответствие с ним в течение двух лет после вступления его в силу. Данный документ является не рекомендательным, а обязательным актом и подлежит прямому применению в государствах – членах ЕС (ст. 99 Регламента). Как справедливо отмечается в литературе, GDPR значительно увеличивает существующие требования к защите персональных данных, расширяя территорию их действия, права граждан, а также вводя специальные требования для финансовых учреждений [4].

Регламент применяется в отношении обработки персональных данных полностью либо частично при помощи автоматизированных средств, а также в отношении обработки персональных данных иными способами, которые являются частью файловой системы или имеют цель стать частью файловой системы. В соответствии с п. 4 преамбулы Регламента право на защиту персональных данных не является абсолютным правом; его необходимо рассматривать относительно его функции в обществе, оно должно быть уравнено с другими основными правами в соответствии с принципом пропорциональности.

Под термином «обработка» в Регламенте понимается любая операция или набор операций, осуществляемые с персональными данными с применением автоматизированных средств или без таковых, например, сбор, запись, организация, структурирование, хранение, модификация и изменение, извлечение, консультирование, использование, раскрытие посредством передачи, распространение или предоставление иным способом, упорядочение или комбинирование, ограничение, стирание или разрушение. Также действие Регламента распространяется на профилирование, в том числе с использованием самообучаемых компьютерных алгоритмов [8]. Следует особо подчеркнуть, что Регламент применяется в отношении обработки персональных данных субъектов данных, находящихся в ЕС, контролером или обрабатывающим данные лицом, не учрежденными в Союзе, если обработка данных касается: предоставления товаров и услуг субъектам данных в ЕС вне зависимости от того, требуется ли оплата от указанного субъекта данных, или мониторинга их деятельности при условии, что деятельность осуществляется на территории ЕС. Компании-нерезиденты подпадают под действие данного Регламента в том числе если используют официальный язык страны – участницы ЕС как в рамках описания товаров/услуг, так и при оформлении заказов; используют валюту страны – участницы ЕС при расчетах с клиентами; непосредственно указали на сайте, что товары/услуги предлагаются гражданам ЕС [2, с. 8]. Такая экстерриториальность действия Регламента требует его тщательного анализа, поскольку его положения могут быть применены и к российским компаниям.

В первую очередь необходимо определить, что же такое «персональные данные» в соответствии с Регламентом. Под этим термином понимается любая информация, относящаяся к идентифицированному или идентифицируемому физическому лицу (ст. 4 (1) Регламента). К информации, которая позволяет идентифицировать лицо прямо или косвенно, относятся имя, идентификационный номер, сведения о местоположении, идентификатор в режиме онлайн, IP-адрес, данные, полученные при использовании cookie, и т. д. (перечень не является исчерпывающим). Под действие Регламента подпадает и псевдонимизированная информация[2]. Такое определение, как отмечают исследователи, по широте сопоставимо с Законом о персональных данных [1, с. 149–162] и шире определения, сформулированного в отменяемой им Директиве [6, с. 234–254]. Анонимизированная информация, т. е. такая информация, которая не позволяет проводить идентификацию лиц, не подпадает под правовое регулирование Регламента.

При определении того, относится ли информация к конкретному лицу, необходимо учитывать как количественные характеристики получаемой информации, так и качественные (содержание информации, цели, для которых она будет использована). Один и тот же набор данных для одного контролера[3] может подпадать под действие Регламента, а для другого – нет.

[2] Под термином «псевдонимизация» понимается обработка персональных данных таким образом, что они не могут быть больше отнесены к определенному субъекту данных без использования дополнительной информации, при условии, что дополнительная информация хранится отдельно и подлежит техническим и организационным мерам, гарантирующим, что персональные данные не отнесены к идентифицированному или идентифицируемому физическому лицу.

[3] Под термином «контролер» понимается физическое или юридическое лицо, органы государственной власти, агентство или иной орган, который самостоятельно или совместно с другими определяет цели и способы обработки персональных данных.

Недостатком Регламента представляется то обстоятельство, что к персональным данным отнесена информация, которая косвенно может идентифицировать лицо. Такая ситуация создает правовую неопределенность в режиме данных и обусловливает отнесение этой информации к сфере регулирования Регламента [7].

В статье 5 Регламента закреплены 7 основных принципов обработки персональных данных: законность, справедливость и прозрачность; ограничение; минимизация данных; точность; ограничение хранения; целостность и конфиденциальность; ответственность (подотчетность).

Законность подразумевает, что данные обрабатываются по основаниям, закрепленным в Регламенте: субъект данных дал согласие на обработку своих персональных данных для одной или нескольких конкретных целей; обработка необходима для исполнения договора, в котором субъект данных является одной из сторон, или для принятия мер по требованию субъекта данных до заключения договора; обработка необходима для соблюдения юридической обязанности, объектом которой является контролер; обработка необходима для защиты жизненных интересов субъекта данных или другого физического лица. Соблюдение принципа законности подразумевает также недопустимость незаконных операций с персональными данными.

При обработке персональных данных принцип справедливости должен соблюдаться наравне с принципом законности, поскольку при нарушении принципа справедливости деятельность по обработке персональных данных будет признана нарушающей Регламент. В силу принципа справедливости контролер или обрабатывающее данные лицо[4] должны обращаться с персональными данными таким способом, который от них будет ожидать разумный человек, и не использовать их таким способом, который оказал бы какой-либо негативный эффект. Для соблюдения принципа справедливости имеет значение не только как осуществляется обработка, но и как была получена информация. Например, если она была получена в большем объеме, чем необходимо, путем введения лица в заблуждение при даче им согласия, то, несмотря на законность обработки, она очевидно будет несправедливой. Иногда информация может использоваться для оказания негативного воздействия на лицо, например, налоговыми органами, но в таком случае невозможно говорить о несправедливости использования информации, поскольку исполняются публичные функции государственного органа.

Прозрачность обработки данных непосредственно связана со справедливостью и подразумевает, что процесс обработки должен быть понятным, открытым и честным. Принцип прозрачности подразумевает, что субъект персональных данных должен быть извещен о том, для каких целей будут собираться и обрабатываться его персональные данные и какие именно. Особое значение соблюдение этого принципа имеет для контролеров и операторов, использующих в своей деятельности *cookie*, поскольку теперь недостаточно лишь обозначить факт их использования и спросить согласие пользователя, необходимо отразить конкретные цели сбора и способы обработки персональных данных. Важно отметить, что сбор и обработка персональных данных не должны начинаться до момента, пока пользователь не согласится на такую обработку, поскольку в ч. 3 ст. 7 Регламента речь идет именно о предварительном согласии.

Принцип целевого ограничения состоит в том, что данные собираются для определенных, явных и законных целей и в дальнейшем не должны обрабатываться несовместимым с этими целями способом. Следовательно, контролер или обрабатывающее данные лицо должен ясно обозначить пользователю, для каких целей собирает и планирует использовать персональные данные, а также отразить это в документации, предусмотренной ст. 30 Регламента[5]. Важно понимать, что нельзя обрабатывать данные способом и для целей, которые не предусмотрены соответствующей документацией, не совместимы с первоначальной целью и о которых не уведомлен пользователь (и не получено его согласие), кроме ряда исключений: для публичных интересов, научных или исторических исследований, статистических целей (ст. 89(1)

[4] Под термином «обрабатывающее данные лицо» понимается физическое или юридическое лицо, органы государственной власти, агентство или иной орган, который обрабатывает персональные данные от имени контролера.

[5] Следует подчеркнуть, что правила о необходимости документации не применяются в отношении предприятий или организаций, на которых занято менее 250 человек, кроме случаев, когда осуществляемая ими обработка может повлечь возникновение риска для прав и свобод субъектов данных, обработка не носит случайный характер или включает специальные категории данных.

Регламента). Эти три цели считаются априори совместимыми с первоначальной целью сбора и обработки персональных данных. Следует подчеркнуть, что Регламент не определяет пределы совместимости целей обработки персональных данных, в связи с чем при определении такой совместимости необходимо учитывать связь между новой и первоначальной целью, характер персональных данных, последствия для пользователя при появлении новой цели обработки и т. д.

В соответствии с принципом минимизации данных лицо должно обрабатывать и собирать персональные данные адекватно (в достаточном количестве для обозначенных целей); персональные данные должны быть соответствующими заявленной цели (предполагается разумная связь данных в целях их обработки); сбор персональных данных должен быть ограничен тем количеством, которое необходимо для заявленных целей. В соответствии с этим принципом недопустимо собирать слишком большое количество информации о пользователях в надежде, что она когда-нибудь пригодится. Более того, согласно ст. 25 Регламента контролер должен имплементировать соответствующие технические и организационные меры для обеспечения того, что по умолчанию обрабатываются только те персональные данные, которые необходимы для каждой конкретной цели обработки.

Принцип точности говорит сам за себя – персональные данные должны быть точными, т. е. соответствующими действительности и, при необходимости, актуальными. В связи с этим необходимо принимать обоснованные и разумные меры для того, чтобы гарантировать своевременное удаление или исправление неточных данных с учетом целей, для которых они обрабатываются. Обрабатывающее данные лицо обязано осуществлять разумные действия для того, чтобы хранимые им персональные данные были точными, а в случае обнаружения неточностей – удалить их или исправить в кратчайшие сроки. Следует отметить, что требования к точности данных связаны с целью их сбора и обработки: например, для статистических или исторических целей последующее изменение персональных данных не имеет существенного значения.

В соответствии с принципом ограничения хранения данные должны храниться в форме, которая позволяет идентифицировать субъектов данных, в течение срока, необходимого для целей, для которых обрабатываются персональные данные. Согласно п. 39 Преамбулы срок хранения персональных данных должен быть ограничен строгим минимумом. Они могут храниться в течение более длительного срока, если будут обрабатываться исключительно в целях общественного интереса, в целях научного или исторического исследования, а также в статистических целях. Следует отдельно подчеркнуть, что это ограничение не распространяется на анонимизированные данные. Соблюдение принципа ограничения хранения позволяет обрабатывающему данные лицу быть уверенным в том, что они точны и соответствуют требованиям других принципов. Политику сроков хранения и удаления информации необходимо также отразить в соответствующих документах организации. Регламент не устанавливает минимальные и максимальные сроки хранения персональных данных, следовательно, обрабатывающее данные лицо или контролер обязаны обосновать соответствующие сроки с учетом целей сбора и обработки персональных данных.

В соответствии с принципом целостности и конфиденциальности (иначе называемым принципом безопасности) персональные данные должны обрабатываться способом, гарантирующим соответствующую безопасность персональных данных, включая защиту от несанкционированной или незаконной обработки и от случайной потери, разрушения или уничтожения данных, с использованием соответствующих технических и организационных мер. Речь идет о так называемом риск-ориентированном подходе к сбору и обработке персональных данных [3, с. 49]. Этот принцип более подробно раскрывается в ст. 32 (1) Регламента, согласно которой контролер и обрабатывающее данные лицо с учетом уровня развития технологий должны имплементировать соответствующие технические и организационные меры, чтобы гарантировать соразмерный риску уровень безопасности, включая inter alia следующее: (a) псевдонимизацию и криптографическую защиту персональных данных; (b) способность гарантировать постоянную конфиденциальность, целостность, доступность и устойчивость систем и услуг, связанных с обработкой; (c) способность своевременно восстанавливать доступность и доступ к персональным данным в случае возникновения инцидента физического или технического свойства; (d) процедуру регулярной проверки и оценки эффективности технических и организационных

мер для обеспечения безопасности обработки. Требования принципа безопасности направлены на предотвращение вреда субъектам, чьи персональные данные собираются и обрабатываются, в частности, от: кражи личности; кражи данных кредитных карт; мошенничества с ипотекой; раскрытия данных о свидетелях и жертвах преступлений и др. Регламент не содержит указаний на уровень безопасности, который необходимо обеспечить, что создает неопределенность: непонятно, какой уровень безопасности необходим для признания его соответствующим закону. Согласно п. 83 Преамбулы для того, чтобы обеспечить безопасность и предотвратить обработку в нарушение Регламента, контролер или обрабатывающее данные лицо должно оценить риски, присущие обработке, и имплементировать меры по снижению указанных рисков, например, криптографическую защиту. При оценке риска для защиты данных необходимо уделить внимание рискам, имеющим место при их обработке, например, случайному или незаконному уничтожению, потере, изменению, несанкционированному раскрытию или доступу к переданным, сохраненным или иным образом обрабатываемым данным, которые могут привести к физическому, материальному или нематериальному ущербу.

В соответствии с п. 81 Преамбулы, чтобы гарантировать соблюдение требований Регламента в отношении обработки, осуществляемой обрабатывающим данные лицом от имени контролера, при возложении на указанное лицо данной обязанности контролер должен использовать обрабатывающих данные лиц, которые предусматривают соответствующие гарантии, в частности, в отношении экспертных знаний, надежности и ресурсов, для того чтобы имплементировать технические и организационные меры, которые будут отвечать требованиям Регламента, в том числе в отношении безопасности обработки. Соблюдение обрабатывающим данные лицом утвержденных норм поведения или сертификационного механизма может использоваться в качестве подтверждения соблюдения обязанностей контролера.

В данном случае в Регламенте речь идет о нескольких подлежащих оценке уровнях безопасности: физической безопасности объекта (качество дверей и надежность замков; наличие камер наблюдения; процедуры допуска сотрудников на объект; процедуры уничтожения бумаг и электронных данных) и кибербезопасности объекта (защита систем – сети и компьютеров в целом; защита данных – информации, размещенной на устройствах; сетевая защита – как самого вебсайта, так и иных любых сетевых сервисов или приложений, наряду с самими сетевыми каналами; защита устройств – например, в некоторых организациях может быть запрещено приносить свои носители информации). Необходимо также учитывать и расходы, которые повлечет имплементация подобных мер безопасности.

Меры безопасности должны соответствовать сложившейся практике организации (например, если в организации допускается удаленный труд, требуется обеспечить соответствующий уровень безопасности при работе с персональными данными, дома у работника), а также природе персональных данных и вреду, который может нанести их утечка субъекту персональных данных.

В соответствии с принципом ответственности, или подотчетности, как его называют исследователи, выраженным в п. 2 ст. 5 Регламента, контролер несет ответственность за соблюдение всех перечисленных принципов и должен быть в состоянии продемонстрировать это. Цель принципа ответственности (подотчетности) состоит в трансформации остальных принципов обработки персональных данных в эффективные механизмы, обеспечивающие реальную защиту [5, с. 176]. Этот принцип состоит из двух отдельных элементов: ответственности за соблюдение Регламента (т. е. контролер должен предпринимать все необходимые и разумные меры для соблюдения требований и принципов Регламента) и необходимости продемонстрировать это соблюдение (например, путем разработки соответствующей политики конфиденциальности, должностных инструкций и т. д.).

Соблюдение этого принципа имеет важное значение, поскольку в соответствии со ст. 83 Регламента при привлечении к ответственности за нарушение требований Регламента в ходе обработки персональных данных будет учитываться в том числе и степень добросовестности контролера или обрабатывающего данные лица. Согласно ст. 24 Регламента контролер должен имплементировать соответствующие технические и организационные меры, гарантирующие и подтверждающие, что обработка осуществляется в соответствии с Регламентом. Следование утвержденным в ст. 40 Регламента нормам поведения или утвержденным в соответствии

со ст. 42 Регламента сертификационным механизмам может быть использовано в качестве элемента для подтверждения соблюдения обязанностей контролера. Если контролер не самостоятельно собирает и обрабатывает персональные данные, то в договоре с обрабатывающим данные лицом необходимо отразить права, обязанности и ответственность последнего. Для демонстрации соблюдения всех принципов в соответствии со ст. 30 Регламента каждый контролер (в определенных случаях представитель контролера) должен вести учет всей деятельности, связанной с обработкой данных и подпадающей под его ответственность. Учетные сведения должны содержать следующую информацию: (a) фамилию и контактные сведения контролера и, в соответствующих случаях, контролера, осуществляющего обработку совместно с ним, представителя контролера и инспектора по защите персональных данных; (b) цели обработки; (c) описание категорий субъектов данных и категорий персональных данных; (d) категории получателей, которым были или будут раскрыты персональные данные, включая получателей в третьих странах или международных организациях; (e) в соответствующих случаях, передачи персональных данных третьей стране или международной организации, включая идентификационные данные указанной третьей страны или международной организации и документальное подтверждение надлежащих гарантий; (f) при наличии возможности, предусмотренные сроки для уничтожения различных категорий данных; (g) при наличии возможности, общее описание технических и организационных мер безопасности и др. Кроме того, в случаях, предусмотренных Регламентом, контролер и обрабатывающее данные лицо должны назначить инспектора по защите персональных данных.

Таким образом, принципы обработки персональных данных, закрепленные в GDPR, легли в основу и нашли отражение во всех предусмотренных Регламентом механизмах, направленных на защиту персональных данных при их сборе и обработке. Принимая во внимание то обстоятельство, что GDPR распространяет свое действие на любого контролера или обрабатывающее данные лицо, подчеркнем, что соблюдение этих принципов необходимо как в рамках ЕС, так и за его пределами, поскольку их нарушение может повлечь соответствующую ответственность. Следует согласиться, что GDPR была принята не для оптимизации функционирования рынка, но для защиты частных интересов субъектов персональных данных, что в итоге может повлиять на рынок, при этом такое влияние неоднозначно и не всегда положительно [7].

### *Список литературы*

1. Грибанов А. А. Общий регламент о защите персональных данных (General Data Protection Regulation): идеи для совершенствования российского законодательства // Закон. 2018. № 3. С. 149–162.

2. Жердина С., Двенадцатова Т., Чмыхов В. Регламент ЕС о персональных данных // ЭЖ-Юрист. 2017. № 33. С. 8–13.

3. Ким Е. Защита ПДн по-европейски // Банковское обозрение. 2017. № 8. С. 48–50.

4. Кроу Д., Кнойпнер Г., Маркштайнер Л. Концепт DPO согласно GDPR: основные принципы создания должности уполномоченного в банке // Банковское обозрение. Приложение «БанкНадзор». 2018. № 1. С. 36–40.

5. Крылова М. С. Принципы обработки персональных данных в праве Европейского союза // Актуальные проблемы российского права. 2017. № 10. С. 175–181.

6. Постникова Е. В. Некоторые аспекты правового регулирования защиты персональных данных в рамках внутреннего рынка Европейского союза // Право. Журнал Высшей школы экономики. 2018. № 1. С. 234–254.

7. Drexl J. Legal Challenges of the Changing Role of Personal and Non-Personal Data in the Data Economy // Max Planck Institute for Innovation & Competition Research Paper. 2018. № 18–23.

8. Kamarinou D., Millard C., Singh J. Machine Learning with Personal Data // Queen Mary School of Law Legal Studies Research Paper. 2016. № 247.

### *References*

1. Gribanov A. A. Obshchii reglament o zashchite personal'nykh dannykh (General Data Protection Regulation): idei dlya sovershenstvovaniya rossiiskogo zakonodatel'stva [General Data Protection Regulation: Ideas for Improvement of Russian Legislation]. *Zakon*, 2018, no. 3, pp. 149–162.

2. Zherdina S., Dvenadtsatova T., Chmykhov V. Reglament ES o personal'nykh dannykh [EU Personal Data Regulations]. *EZh-Yurist*, 2017, no. 33, p. 8–13.

3. Kim E. Zashchita PDn po-evropeiski [PD Protection in a European Way]. *Bankovskoe obozrenie – Banking Review,* 2017, no. 8, pp. 48–50.

4. Krou D., Knoipner G., Markshtainer L. Kontsept DPO soglasno GDPR: osnovnye printsipy sozdaniya dolzhnosti upolnomochennogo v banke [The Concept of DPO According to the GDPR: the Basic Principles of Creating a Position Authorized in the Bank]. *Bankovskoe obozrenie. Prilozhenie "BankNadzor" – Banking Review. Application "BankNadzor",* 2018, no. 1, pp. 36–40.

5. Krylova M. S. Printsipy obrabotki personal'nykh dannykh v prave Evropeiskogo soyuza [Principles of Processing Personal Data in the European Union Law]. *Aktual'nye problemy rossiiskogo prava – Actual Problems of Russian Law*, 2017, no. 10, pp. 175–181.

6. Postnikova E. V. Nekotorye aspekty pravovogo regulirovaniya zashchity personal'nykh dannykh v ramkakh vnutrennego rynka Evropeiskogo soyuza [Aspects of Legal Regulation of Protecting Personal Data in the EU Internal Market]. *Pravo. Zhurnal Vysshei shkoly ekonomiki – Law. Journal of the Higher School of Economics*, 2018, no. 1, pp. 234–254.

7. Drexl J. Legal Challenges of the Changing Role of Personal and Non-Personal Data in the Data Economy. *Max Planck Institute for Innovation & Competition Research Paper*, 2018, no. 18–23.

8. Kamarinou D., Millard C., Singh J. Machine Learning with Personal Data. *Queen Mary School of Law Legal Studies Research Paper*, 2016, no. 247.