М. С. Крылова*

Принципы обработки персональных данных в праве Европейского Союза

Аннотация. *В настоящей статье рассмотрены принципы обработки персональных данных, установленные в законодательстве Европейского Союза. Рассмотрены их общие особенности, а также сущность и специфика применения каждого принципа в отдельности. Установлены основные системные взаимосвязи между принципами. Кроме того, в статье отражены основные новации принятого в процессе реформирования законодательства ЕС об охране персональных данных Регламента (ЕС) 2016/679 о защите физических лиц при обработке персональных данных и о свободном движении таких данных, коснувшиеся принципов обработки персональных данных.*

Ключевые слова: *принципы, обработка персональных данных, Европейский Союз, правовая охрана персональных данных, реформирование законодательства.*

DOI: 10.17803/1994-1471.2017.83.10.175-181

ВВЕДЕНИЕ

На сегодняшний день в Европейском Союзе (далее — ЕС) базовый перечень принципов обработки персональных данных установлен в принятой в 1995 г. Директиве 95/46/ЕС о защите физических лиц при обработке персональных данных и о свободном движении таких данных[1] (далее — Директива 1995 г.). В 2016 г. после продолжительного периода подготовки по итогам пересмотра основных концептуальных положений данной Директивы и законодательства об охране персональных данных в целом был принят Регламент (ЕС) 2016/679 о защите физических лиц при обработке персональных данных и о свободном движении таких данных[2] (далее — Регламент 2016 г.). Он будет применяться в государствах — членах ЕС с 27 мая 2018 г.

Несмотря на то что реализация имплементированных положений Директивы 1995 г. на национальном уровне в некоторых случаях

[1] 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 // OJ L 281. 23.11.1995. P. 0031-0050.

[2] 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) // OJ L 119. 04.05.2016. P. 1—88.

* *Крылова Мария Сергеевна*, соискатель кафедры интеграционного и европейского права Московского государственного юридического университета имени О.Е. Кутафина (МГЮА)
mariya.s.krylova@gmail.com
125993, Россия, г. Москва, ул. Садовая-Кудринская, д. 9

была признана неудовлетворительной[3], в ЕС почти повсеместно признается, что сформулированные в ней принципы теоретически обоснованы и обладают достаточной гибкостью. Однако, принимая во внимание эволюцию методов автоматической обработки информации и необходимость соответствия правового регулирования глобальным тенденциям развития сферы информационных технологий, в ходе реформирования Директива 1995 г. подверглась значительным изменениям. Учитывая основополагающую роль принципов обработки персональных данных, особую актуальность приобретает рассмотрение внесенных в данный сегмент регулирования изменений.

Всего в Регламенте 2016 г. выделены семь принципов обработки персональных данных: принцип правомерности, справедливости и прозрачности; принцип ограниченного целевого назначения; принцип минимизации данных; принцип корректности данных; принцип ограниченного хранения; принцип целостности и конфиденциальности; принцип подотчетности.

ПРИНЦИП ПРАВОМЕРНОСТИ, СПРАВЕДЛИВОСТИ И ПРОЗРАЧНОСТИ

Несмотря на то что требования правомерности, справедливости и прозрачности закреплены в ст. 5 Регламента 2016 г. в рамках единого принципа, в других разделах Регламента и доктринальных источниках они часто рассматриваются как отдельные принципы[4].

В отношении правомерности обработки персональных данных в Регламенте 2016 г. содержится четкое положение: чтобы обработка являлась правомерной, должно быть соблюдено, по крайней мере, одно из законодательно установленных семи оснований правомерности[5]. Рассматривая их, можно условно дифференцировать наличие согласия субъекта данных от остальных оснований, так как в данном случае условием правомерности обработки персональных данных выступает волеизъявление субъекта данных. Все другие основания, напротив, позволяют производить обработку данных в случаях, когда она целесообразна и необходима в целях защиты законных интересов других лиц[6]. В контексте применения принципа правомерности согласие лица на обработку данных имеет важное значение, но «не отменяет обязательств контролера в отношении справедливости, необходимости, соразмерности, а также качества обработки данных»[7], т.е. не освобождает его от соблюдения других принципов обработки персональных данных.

Справедливость обработки персональных данных обычно рассматривается в совокупности либо с принципом правомерности, либо с принципом прозрачности. В сущности, «несправедливой» обработку персональных данных делает отсутствие о ней достаточной информации, т.е. «если субъекту данных предоставляется неполноценная информация, и это ставит его в положение невозможности самостоятельно распоряжаться своими персональными данными»[8]. Сто́ит обратить внимание, что в результате реформы понимание справедливости обработки персональных данных стало несколько размытым. Не последнюю роль в этом сыграло введение принципа прозрачности, отсутствовавшего в Директиве 1995 г.

---

[3] Report from the Commission. First report on the implementation of the Data Protection Directive (95/46/EC) // COM(2003) 265 final. Brussels. 15.05.2003.

[4] См.: подробнее: Регламент (ЕС) 2016/679, п. 39, 45, 58, 60, 71, 78, 100 преамбулы, п. 2—3 ст. 6, п. 2 ст. 14, ст. 40 ; *Savin A.* EU Internet Law. Edward Elgar Publishing Limited, 2013. P. 216 ; *Fuster G. G.* The Emergence of Personal Data Protection as a Fundamental Right of the EU. Springer, 2014. P. 4, 204 ; *Lynskey O.* The Foundations of EU Data Protection Law. Oxford University Press, 2015. P. 129, 260.

[5] Регламент (ЕС) 2016/679. Ст. 6.

[6] См.: Article 29 Working Party Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC // 844/14/EN, WP 217. 09.04.2014.

[7] Article 29 Working Party Opinion 15/2011 on the definition of consent // 01197/11/EN, WP187, 13.07.2011. P. 7.

[8] *Maxwell W. J.* A comparative look at «fair processing» under European and U.S. data protection law // Quelle protection des données personnelles en Europe? Céline Castets-Renard (ed.), University of Toulouse. Larcier, 2015. P. 141.

До реформирования законодательства об охране персональных данных требование прозрачности обработки персональных данных косвенно подразумевалось, однако его нормативное закрепление в перечне принципов стало одной из новаций Регламента 2016 г. В результате в соответствии с Регламентом 2016 г. прозрачность обработки персональных данных предполагает, чтобы «любая информация, адресованная общественности или субъекту данных, была краткой, легко доступной, несложной для восприятия, чтобы использовался четкий и понятный язык и, при необходимости, с применением визуализации»[9].

Таким образом, справедливость обработки персональных данных напрямую зависит от количественной и содержательной характеристик информации, предоставляемой субъекту данных в отношении операций, производимых с его персональными данными, в то время как прозрачность больше акцентирует внимание на доступности для субъекта данных такой информации и форме ее представления.

ПРИНЦИП ОГРАНИЧЕННОГО ЦЕЛЕВОГО НАЗНАЧЕНИЯ

Принцип ограниченного целевого назначения играет важную роль в правовом регулировании обработки персональных данных, так как выступает предварительным условием для применения остальных принципов.

Учрежденный в соответствии с Директивой 1995 г. вспомогательный орган ЕС на уровне экспертов государств-членов («Рабочая группа 29 статьи») определяет данный принцип как совокупность двух компонентов: «спецификации целей» (англ. purpose specification) и «совместимого использования» (англ. compatible use). При определении целей имеет важное значение их легитимность, которая в первую очередь должна быть подтверждена в контексте перечня оснований правомерности. Однако нужно учитывать, что «спецификация целей и требование иметь законное основание для обработки персональных данных являются двумя отдельными требованиями, рассматриваемыми в совокупности»[10]. Также лицом, осуществляющим обработку персональных данных, должны быть приняты все необходимые меры для четкого, полного и недвусмысленного понимания субъектом данных целей обработки (в соответствии с принципом прозрачности).

Анализируя второй элемент принципа ограниченного целевого назначения — «совместимое использование», сто́ит отметить, что в случае отсутствия согласия субъекта данных при дальнейшей обработке личной информации возникает необходимость определения совместимости новых целей с первоначальными. Несовместимость таких целей даже при наличии основания правомерности влечет за собой прямое нарушение принципа ограниченного целевого назначения.

Отсутствие в Директиве 1995 г. положений о методике выявления несовместимости целей было в значительном объеме восполнено Регламентом 2016 г., где теперь установлено, какие именно факторы контролеру нужно учитывать при определении совместимости целей. В их число входят: наличие связи между целями предполагаемой обработки и первоначальными целями; специфика сбора персональных данных и категория, к которой они относятся; возможные последствия дальнейшей обработки; наличие соответствующих гарантий, например, шифрования или псевдонимизации[11].

ПРИНЦИП МИНИМИЗАЦИИ ДАННЫХ

В сущности, принцип минимизации данных налагает на контролеров обязанность собирать только те данные, которые отвечают поставленной цели обработки, и хранить их только в течение того времени, которое требуется для реализации поставленной цели обработки[12]. Зависимость минимизации данных от целей обработки говорит о прочной связи данного принципа с принципом ограниченного целевого назначения.

[9] Регламент (ЕС) 2016/679. П. 58 преамбулы.

[10] Article 29 Working Party Opinion 03/2013 on purpose limitation // 00569/13/EN, WP203. 02.04.2013. P. 11—13.

[11] Регламент (ЕС) 2016/679. П. 4 ст. 6.

[12] См.: Регламент (ЕС) 2016/679. Пп. (c) п. 1 ст. 5, п. 78, 156 преамбулы.

Кроме того, минимизация данных является одним из методов, используемых в рамках концепции «проектируемой защиты данных»[13] (англ. privacy by design, фр. protection des données dès la conception), которая предполагает наличие в программном обеспечении и других технических разработках изначально встроенных мер защиты персональных данных.

Следовательно, рассматриваемый принцип выступает в отношении защиты данных в качестве меры предупредительного характера, что отвечает тенденциям развития правового регулирования обработки персональных данных. В частности, одной из таких тенденций выступает формирование базиса для комплексной защиты личной информации, который совмещает в себе технические и организационные меры, применяемые как непосредственно в процессе обработки персональных данных, так и на этапе создания соответствующих систем. По существу, это взаимодействие концепций «проектируемой защиты данных» и «защиты данных по умолчанию» (англ. privacy by default, фр. protection des données par défaut)[14].

Для демонстрации соответствия требованиям Регламентом 2016 г. были предусмотрены процедуры добровольной сертификации[15].

ПРИНЦИП КОРРЕКТНОСТИ ДАННЫХ

Принцип корректности данных основывается на предъявляемом к личной информации в процессе обработки требовании точности, полноты и актуальности. Указанные характеристики должны быть обеспечены в той мере, в какой это необходимо для выполнения конкретных целей. В данном случае взаимосвязь с принципом ограниченного целевого назначения проявляется так же, как и в ситуации с другими принципами: цели обработки выступают формирующим фактором по отношению к искомым характеристикам информации.

Осуществление данного принципа выступает основанием предоставления субъекту данных прав на исправление, удаление или дополнение его персональных данных. Указанные права способствуют достижению точности, полноты и актуальности личной информации. «Предоставление субъектам данных прав, благодаря которым они будут играть активную роль в управлении своими персональными данными, может быть единственным эффективным методом предупреждения злоупотреблений и ненадлежащего использования данных со стороны других лиц»[16]. В целом, чтобы получить более точные данные, должны использоваться регулярные средства контроля и исправления[17].

Обеспечение и поддержание корректности и согласованности данных на протяжении всего их жизненного цикла является определением целостности данных[18]. Таким образом проявляется взаимосвязь рассматриваемого принципа с принципом целостности и конфиденциальности.

ПРИНЦИП ОГРАНИЧЕННОГО ХРАНЕНИЯ

Принцип ограниченного хранения означает, что «персональные данные должны храниться в форме, позволяющей производить идентификацию субъектов данных, не дольше, чем этого требует достижение целей, для которых

---

[13] См.: подробнее: Регламент (ЕС) 2016/679. П. 1 ст. 25 ; Article 29 Working Party. The Future of Privacy// 02356/09/EN, WP168, 01.12.2009.

[14] См.: Регламент (ЕС) 2016/679. П. 2 ст. 25.
Подробнее о данных концепциях см.: *Cavoukian A.* Privacy by Design: Leadership, Methods, and Results / Gutwirth S., Leenes R., de Hert P., Poullet Y. (eds.) // European Data Protection: Coming of Age. Springer, 2013. P. 175—202.

[15] См.: Регламент (ЕС) 2016/679. П. 3 ст. 25, ст. 42.

[16] *Cavoukian A.* Privacy by Design: Leadership, Methods, and Results / Gutwirth S., Leenes R., de Hert P., Poullet Y. (eds.) // European Data Protection: Coming of Age. Springer, 2013. P. 183.

[17] См.: *Čas J.* Ubiquitous Computing, Privacy and Data Protection: Options and Limitations to Reconcile the Unprecedented Contradictions / Gutwirth S., Leenes R., de Hert P., Poullet Y. (eds.) // Computers, Privacy and Data Protection: an Element of Choice. Springer, 2011. P. 152.

[18] См.: Cyber Security and Privacy. Trust in the Digital World and «Cyber Security and Privacy EU Forum» / Felici M. (ed.). Brussels. Springer, 2013. P. 24.

обрабатываются персональные данные»[19]. «Однако ограничение хранения персональных данных по времени применяется только к той информации, которая позволяет производить идентификацию субъектов данных. Таким образом, правомерное хранение не нужной более информации+ может быть осуществлено путем анонимизации данных или псевдонимизации»[20]. Кроме того, в некоторых установленных законом случаях (например, при обработке персональных данных в сфере уголовно-правового регулирования; в целях архивации (в общественных интересах), в целях научных и исторических исследований или в статистических целях) персональные данные могут храниться в течение более длительных периодов времени.

В контексте применения данного принципа необходимо обратить внимание на важную новацию Регламента 2016 г.: «право на забвение» (англ. right to be forgotten; фр. droit à l'oubli). Первоначально данная концепция получила свое развитие в судебной практике Суда ЕС. Суть ее заключается в предоставлении субъекту данных права на удаление при определенных условиях его личной информации из общедоступных источников (в частности, поисковых систем). Указанное право применяется в отношении «некорректной, неактуальной, нерелевантной, избыточной в соответствии с целями обработки информации»[21]. В то же время при реализации данного права должен быть соблюден баланс с другими фундаментальными категориями: свободой выражения мнений и свободой массовой информации[22].

ПРИНЦИП ЦЕЛОСТНОСТИ И КОНФИДЕНЦИАЛЬНОСТИ

В сущности, понятия целостности и конфиденциальности являются частью классической AIC-триады[23] (англ. Availability, Integrity, Confidentiality), которая используется при построении систем защитных мер и механизмов информационной безопасности организаций. Данная концепция всегда выступает базовым элементом таких систем, несмотря на то, что ее компоненты применяются в разном соотношении в зависимости от организационной структуры и целевой направленности организации.

Принцип целостности и конфиденциальности предусматривает «осуществление надлежащих технических и организационных мер для обеспечения уровня безопасности, соответствующего возможным рискам»[24] при работе с персональными данными. Эти условия должны способствовать предотвращению несанкционированных операций с персональными данными в результате как незаконного вмешательства (с помощью вредоносного программного обеспечения), так и непреднамеренного (в связи с ошибкой администратора базы данных).

Для этой цели Регламент 2016 г. предусматривает использование следующих инструментов: «псевдонимизации и шифрования персональных данных; обеспечения постоянной конфиденциальности, целостности, доступности и устойчивости систем обработки персональных данных и соответствующего оборудования; способности своевременно восстанавливать доступ к персональным данным в случае физического или технического происшествия; регулярного тестирования в процессе управления данными, оценки эффективности технических и организационных мер для обеспечения безопасности обработки»[25].

Кроме того, фундаментальное значение, которое имеет обеспечение безопасности данных, послужило причиной того, что в процессе реформы соответствующее требование было включено в перечень принципов обработки персональных данных.

---

19 Регламент (ЕС) 2016/679. Ст. 5.

20 Handbook on European data protection law // EU Agency for Fundamental Rights and Council of Europe. Belgium, 2014. P. 73.

21 Case C-131/12 Google Spain v Agencia Española de Protección de Datos (AEPD) and Mario Costeja Gonzalez. ECLI:EU:C:2014:317. Para 93.

22 См.: Case C-131/12 Google Spain v Agencia Española de Protección de Datos (AEPD) and Mario Costeja Gonzalez. ECLI:EU:C:2014:317. Para 85 ; Регламент (ЕС) 2016/679. П. 65 преамбулы.

23 См.: *Whitman M. E., Mattord H. J.* Principles of Information Security. Cengage Learning, 6th ed. 2017. P. 11.

24 Регламент (ЕС) 2016/679. Ст. 32.

25 Регламент (ЕС) 2016/679. Ст. 32.

ПРИНЦИП ПОДОТЧЕТНОСТИ

Особая роль принципа подотчетности проявляется в его положении в системе принципов обработки персональных данных: в Регламенте 2016 г. он дифференцирован от других принципов и закреплен в п. 2 ст. 5. Разумеется, это обусловлено сущностными характеристиками принципа как элемента системы, задачей которого является обеспечение контроля за соблюдением остальных принципов. Принцип подотчетности не был закреплен в законодательных актах ЕС в области обработки персональных данных до принятия Регламента 2016 г., однако фактически требования, составляющие его основу, уже были установлены Директивой 1995 г. «С этой точки зрения положение о подотчетности не представляет большой новизны, и по большей части оно не накладывает требований, которые еще не были включены в существующее законодательство»[26].

Цель принципа подотчетности состоит в трансформации остальных принципов обработки персональных данных в эффективные механизмы, обеспечивающие реальную защиту. В схематическом виде понятие подотчетности сосредоточено на двух основных элементах: «необходимость принятия контролером надлежащих и эффективных мер для реализации принципов обработки данных; необходимость продемонстрировать по запросу, что были приняты надлежащие и эффективные меры»[27]. Однако в случае, если учетные записи, которые составляют основу процедуры отчетности, сами включают персональные данные, возникает конфликт принципов отчетности и минимизации данных, так как это вызывает увеличение общего количества обрабатываемой личной информации[28].

Сильное влияние на реализацию подотчетности оказывает принцип прозрачности обработки персональных данных. Ведь в целом «системы прозрачности изначально задумываются как системы подотчетности по причине столкновения с классической проблемой того, перед кем подотчетны отчитывающиеся»[29]. Таким образом, в результате реализации принципа прозрачности, в частности, путем публикации политики конфиденциальности в сети Интернет, представления ежегодных докладов, а также с помощью обеспечения прозрачности в отношении внутренних процедур подачи жалоб в отношении связанных с обработкой персональных данных ситуаций, достигается более высокий уровень подотчетности[30].

ЗАКЛЮЧЕНИЕ

Принципы обработки персональных данных образуют систему взаимосвязанных элементов, в рамках которой предусмотрен комплексный подход к определению каждого принципа, что способствует повышению эффективности их применения.

Кроме того, изменения, внесенные в результате реформирования законодательства Европейского Союза об охране персональных данных, значительно адаптировали рассматриваемые принципы к современному уровню развития сферы информационных технологий. Однако в настоящее время сложно сделать вывод о том, насколько эффективной станет их практическая реализация.

Таким образом, вопрос толкования принципов обработки персональных данных в праве Европейского Союза является весьма актуальным и требует дальнейшего изучения.

---

[26] Article 29 Working Party Opinion 3/2010 on the principle of accountability // 00062/10/EN, WP173, 13.07.2010. Para 36.

[27] Article 29 Working Party Opinion 3/2010 on the principle of accountability. Para 28.

[28] См.: *Butin D., Chicote M., Le Métayer D.* Strong Accountability: Beyond Vague Promises // Reloading Data Protection. Multidisciplinary Insights and Contemporary Challenges. Gutwirth S., Leenes R., de Hert P. (eds.). Springer, 2014. P. 355.

[29] *Regan P. M., Johnson D. G.* Privacy and Trust in Socio-technical Systems of Accountability // Managing Privacy through Accountability / Guagnin D., Hempel L. (eds.). Palgrave Macmillan, 2012. P. 139.

[30] См.: Article 29 Working Party Opinion 3/2010 on the principle of accountability. Para 48.

БИБЛИОГРАФИЯ

1. *Butin D., Chicote M., Le Métayer D.* Strong Accountability: Beyond Vague Promises // Reloading Data Protection. Multidisciplinary Insights and Contemporary Challenges / Gutwirth S., Leenes R., de Hert P. (eds.). — Springer, 2014. — P. 343—369.
2. *Čas J.* Ubiquitous Computing, Privacy and Data Protection: Options and Limitations to Reconcile the Unprecedented Contradictions // Computers, Privacy and Data Protection: an Element of Choice / Gutwirth S., Leenes R., de Hert P., Poullet Y. (eds.). — Springer, 2011. — P. 139—170.
3. *Cavoukian A.* Privacy by Design: Leadership, Methods, and Results / Gutwirth S., Leenes R., de Hert P., Poullet Y. (eds.) // European Data Protection: Coming of Age. — Springer, 2013. — P. 175—202.
4. *Felici M.* (ed.) Cyber Security and Privacy. Trust in the Digital World and «Cyber Security and Privacy EU Forum». — Brussels : Springer, 2013. — 177 p.
5. *Fuster G. G.* The Emergence of Personal Data Protection as a Fundamental Right of the EU. — Springer, 2014. — 284 p.
6. *Maxwell W. J.* A comparative look at «fair processing» under European and U.S. data protection law // Quelle protection des données personnelles en Europe? Céline Castets-Renard (ed.). — University of Toulouse. Larcier, 2015. — P. 137—154.
7. *Lynskey O.* The Foundations of EU Data Protection Law. — Oxford University Press, 2015. — 312 p.
8. *Regan P. M., Johnson D. G.* Privacy and Trust in Socio-technical Systems of Accountability // Managing Privacy through Accountability / Guagnin D., Hempel L. (eds.). — Palgrave Macmillan, 2012. — P. 125—142.
9. *Savin A.* EU Internet Law. — Edward Elgar Publishing Limited, 2013. — 286 p.
10. *Whitman M. E., Mattord H. J.* Principles of Information Security. Cengage Learning. — 6th ed. — 2017. — 728 p.

Материал поступил в редакцию 7 июля 2017 г.

PRINCIPLES OF PROCESSING PERSONAL DATA IN EUROPEAN UNION LAW

KRYLOVA Mariya Sergeevna — Postgraduate of the Department of Integration and European Law, Kutafin Moscow State University
mariya.s.krylova@gmail.com
125993, Russia, Moscow, Sadovaya-Kudrinskaya Str., 9

Abstract. *This article describes the principles to the processing of personal data set out in the European Union legislation. Their common features, as well as the essence and specificity of each principle are considered separately. The basic system of the relationship between the principles is defined. In addition, the article highlights innovations adopted in the process of reforming the EU legislation on the protection of personal data, Regulation (EC) 2016/679 On the Protection of Individuals with regard to the processing of personal data and on the free movement of such data, principles concerning the processing of personal data.*

Keywords: *principles to the processing of personal data, the European Union, the legal protection of personal data, legislation reforms.*