Алексей А. Сиротский
*Национальный исследовательский Московский государственный строительный университет (НИУ МГСУ),*
*Ярославское шоссе, 26, Москва, 129337, Россия*
*e-mail: hotwater2009@yandex.ru, https://orcid.org/0000-0002-9343-7185*

# АНАЛИЗ ИЗМЕНЕНИЙ ЗАКОНОДАТЕЛЬСТВА О ПЕРСОНАЛЬНЫХ ДАННЫХ, ВСТУПАЮЩИХ В СИЛУ С 1 СЕНТЯБРЯ 2022 Г.

*DOI: http://dx.doi.org/10.26583/bit.2022.4.06*

*Аннотация.* В статье проводится анализ нормативно-правовых изменений в требованиях к организациям-операторам персональных данных процессов защиты персональных данных, вступающих в силу с 1 сентября 2022 г. В статье также отмечается, что ряд новых норм также вступит в силу с 1 марта 2023 г. Новые требования содержат ряд ограничений и ужесточений уже существующих процессов защиты персональных данных, а также ряд активных нововведений, требующих внедрение новых процессов, направленных на повышение безопасности персональных данных и оперативное выявление и расследование инцидентов. Каждое изменение и нововведение анализируется по совокупности признаков, включающих выявление нормы закона, исследование новых требований и формирование вывода о сущности изменений и необходимой совокупности действий, направленных на обеспечение исполнения требований. Всего выделено 14 принципиальных и существенных изменений и дополнений в требованиях к защите персональных данных. Наиболее трудоёмким и затратным для предприятий малого бизнеса станет подключение к государственной системе обнаружения, предупреждения и ликвидации последствий компьютерных атак, что потребует привлечения дополнительных средств и сотрудников. Сформулированы первоочередные задачи, которые должны решить организации–операторы персональных данных для обеспечения соответствия новым нормам. Одной из ключевых задач станет формирование группы по расследованию инцидентов информационной безопасности, а также создание системы управления инцидентами информационной безопасности и внедрение программных продуктов, направленных на решение данной задачи. Другой важной задачей является подготовка специалистов, обладающих знаниями и компетенциями, необходимыми для решения новых задач и развитие программ формирования культуры обращения с персональными данными, направленных на широкие слои населения.

*Ключевые слова: персональные данные, организация-оператор, требования безопасности, инциденты, защита данных, подготовка специалистов.*
*Для цитирования: СИРОТСКИЙ, Алексей А. АНАЛИЗ ИЗМЕНЕНИЙ ЗАКОНОДАТЕЛЬСТВА О ПЕРСОНАЛЬНЫХ ДАННЫХ, ВСТУПАЮЩИХ В СИЛУ С 1 СЕНТЯБРЯ 2022 Г. Безопасность информационных технологий, [S.l.], т. 29, № 4, с. 67–81, 2022. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1450. DOI: http://dx.doi.org/10.26583/bit.2022.4.06.*

Alexei A. Sirotskiy
*Federal State Budget Educational Institution of Higher Education «Moscow State University of Civil Engineering (National Research University),*
*Yaroslavskoye shosse, 26, Moscow, 129337, Russia*
*e-mail: hotwater2009@yandex.ru, https://orcid.org/0000-0002-9343-7185*

## Analysis of changes in personal data legislation since September 1, 2022

*DOI: http://dx.doi.org/10.26583/bit.2022.4.06*

*Abstract.* The paper analyzes regulatory and legal changes in the requirements for the organization of personal data by operators of personal data protection processes, which came into force on September 1, 2022. It is noted that a number of additional regulations are also going to come into force on March 1, 2023, although they are not considered in the paper. The new requirements contain a number of restrictions and tightening of existing protecting personal data processes, as well as a number of active innovations requiring

the introduction of new processes aimed at improving the security of personal data and promptly identifying and investigating incidents. Each change and innovation are analyzed by a set of features, including the identification of the law rules, the study of new requirements and the formation of a conclusion about the essence of changes and the necessary set of actions aimed at ensuring the fulfillment of requirements. In total 14 fundamental and significant changes and additions to the requirements for the protection of personal data have been identified. The most time-consuming and costly for small businesses is the link to the state system for detecting, preventing and eliminating the consequences of computer attacks, which requires attracting additional funds and employees. Priority tasks to be solved by the personal data operators in order to ensure compliance with the new standards have been formulated. Those are the building up a team to investigate information security incidents, as well as creation of a system for managing information security incidents and the introduction of software products for solving this problem. Another important task is to train the specialists with the knowledge and competencies necessary to solve new problems and to develop the programs for the personal data management culture formation aimed at the general public.
*Keywords: personal data, organization-operator, security requirements, incidents, data protection, specialists' preparation.*
*For citation: SIROTSKIY, Alexei A. Analysis of changes in personal data legislation since September 1, 2022. IT Security (Russia), [S.l.], v. 29, no. 4, p. 67–81, 2022. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1450. DOI: http://dx.doi.org/10.26583/bit.2022.4.06.*

## Введение

Государственной Думой РФ 6 июля 2022 г. был окончательно принят Федеральный закон № 266-ФЗ «О внесении изменений в Федеральный закон «О персональных данных», отдельные законодательные акты Российской Федерации и признании утратившей силу части четырнадцатой статьи 30 Федерального закона «О банках и банковской деятельности»[1], который был официально опубликован 14 июля 2022 г.

Часть новых положений, устанавливаемых, и впервые вводимых данным законом, вступают в силу с 1 сентября 2022 г., а часть – с 1 марта 2023 г.

Поводом к принятию новых норм и положений в области защиты персональных данных стал анализ инцидентов последних лет, когда персональные данные граждан массово попадали в открытый доступ [1]. Риски несанкционированного распространения конфиденциальной информации увеличиваются в связи с развитием информационных сервисов в цифровой экономике [2], что соответствует современным тенденциям.

Вопросы обеспечения персональной безопасности личности за последние годы только повышают свою актуальность и могут рассматриваться в различных концептуальных проблемах делового оборота [3, 4]. Принятие новых норм направлено на повышение безопасности личности в современной информационной среде [5].

Новые законодательные нормы значительно усиливают государственный контроль над оборотом персональных данных, вводя ряд новых обязанностей для операторов персональных данных, заключающиеся, прежде всего, в необходимости непрерывного взаимодействия с государственными органами власти и уполномоченными структурами.

Всё это повлечёт необходимость в организациях-операторах персональных данных пересмотреть действующие процессы и внести коррективы в модели функционирования систем обеспечения информационной безопасности, приведя их к соответствию новым нормативным требованиям. Вполне вероятно, это потребует от операторов персональных данных провести внеочередной аудит безопасности своей инфраструктуры и бизнес-процессов [6].

По сравнению с законодательными требованиями и практикой защиты персональных данных в коммуникативной среде прошлого периода [7, 8], в настоящее

[1]URL: http://publication.pravo.gov.ru/Document/View/0001202207140080 (дата обращения: 07.09.2022).

время на операторов персональных данных накладываются большие обязанности и более высокая ответственность.

В данной работе проведён анализ наиболее существенных и принципиальных изменений законодательных требований к обработке персональных данных, вступающих в силу с 1 сентября 2022 г., и которые влекут за собой существенные изменения процессов обработки персональных данных в организациях, а также потребуют произвести корректировку и расширение применяемых операторами мер и средств обеспечения защищённости персональных данных [9, 10].

В настоящее время ключевой проблемой является осознание специалистами и сотрудниками компаний и организаций произошедших изменений, понимание новых законодательных требований, выработка подходов к осуществлению изменений в деловых процессах внутри организации и решение задач по приведению процессов обработки персональных данных в соответствии с новыми требованиями.

Целью исследований является анализ изменений законодательства в области защиты персональных данных и формулирование выводов о смысле произошедших изменений и путях достижения соответствия новым требованиям.

Методы исследований опираются на анализе и сопоставлении редакций Федерального Закона №152 «О персональных данных», выявлении ключевых норм, формируемых данным законом, трактовке положений закона, изучении обычаев и практики организационно-правовых решений в области защиты персональных данных, а также изучении и анализе сопроводительной и пояснительной информации, обсуждавшейся на стадии принятия данного закона.

Каждое изменение в данной работе рассматривается отдельно. При этом выделяются следующие характеристики изменений:

– характер нововведения: изменение существующего порядка или введение новых, ранее отсутствовавших норм, понятий и требований;

– статья или часть статьи закона, в которой произошли изменения;

– определение нормы, которой касается изменение и в рамках которой возникают новые требования;

– формулирование требований, существовавших до 1 сентября 2022 г.;

– формулирование требований и норм, возникающих и вступающих в силу с 1 сентября 2022 г.;

– выводы о сущности изменений и сущности новых требований, что станет основой для разработки операторами персональных данных решений и совокупности действий, направленных на обеспечение исполнения рассматриваемых требований.

## Исследование и анализ изменений

Проведём выявление и анализ изменений требований к обработке персональных данных, в соответствии с изменениями Федерального закона №152 «О персональных данных», вступающими в силу с 1 сентября 2022 г.

**Изменение 1.**

Дополнена статья 1 Федерального Закона №152 «О персональных данных».

Ранее, ФЗ-№152 «О персональных данных» был обязателен к применению Российскими юридическими и физическими лицами.

Теперь требования данного закона будут распространяться и на иностранных физических и юридических лиц, которые обрабатывают персональные данные Российских граждан.

Таким образом, вводится экстерриториальность применения российского законодательства о персональных данных. Устанавливается возможность вмешательства уполномоченных органов власти в вопросы обработки персональных данных российских граждан на территории других государств.

**Изменение 2.**

Дополнена статья 4 Федерального Закона №152 «О персональных данных».

Дополнение касается нормы, которая определяет, что Государственные органы, Банк России, органы местного самоуправления могут принимать нормативные правовые акты по вопросам, касающимся обработки персональных данных.

Ранее никаких дополнительных требований по принятию данных подзаконных документов не было.

Теперь эти правовые акты подлежат обязательному согласованию с уполномоченным органом по защите прав субъектов персональных данных в случаях, если они регулируют отношения, связанные с осуществлением трансграничной передачи персональных данных, обработкой специальных категорий персональных данных, биометрических персональных данных, персональных данных несовершеннолетних, предоставлением, распространением персональных данных, полученных в результате обезличивания.

Таким образом, вводится процедура согласования наиболее ответственных нормативных актов с уполномоченным регулятором – Роскомнадзором.

**Изменение 3.**

Дополнен подпункт 5 части 1 статьи 6 Федерального Закона №152 «О персональных данных».

Как известно, обработка персональных данных может проводиться по чётким основаниям, одним из которых является обработка персональных данных для исполнения договора, стороной которого либо выгодоприобретателем или поручителем, по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем. Дополнение содержит ограничения на условия такого договора.

Теперь запрещается:

– ограничивать в договоре права и свободы субъекта персональных данных;

– устанавливать случаи обработки персональных данных несовершеннолетних (если иное не предусмотрено законодательством Российской Федерации);

– определять бездействие субъекта персональных данных как условие возникновения договорных отношений.

Таким образом, наконец, пресекается практика, когда в договоре указывалось, что «отсутствие отказа со стороны субъекта означает его согласие». Можно надеяться, что это сможет положить конец автоматическим подключениям к рекламным рассылкам, платным сервисам (с предоставлением бесплатного периода), и другим взаимодействиям с клиентами в которых ранее предусматривалось «молчаливое» согласие при отсутствии со стороны клиента ярко выраженного отказа.

В отношении обработки персональных данных несовершеннолетних можно отметить, что такое понятие, как «персональные данные несовершеннолетних» появилось в законе впервые. В предыдущих редакциях такого понятия как самостоятельной категории не выделялось в принципе. Процессы, процедуры, основания и возможные задачи обработки персональных данных несовершеннолетних пока не имеют отдельного регулирования и в целом опираются на гражданское законодательство, определяющее для

несовершеннолетних их законных представителей. На текущий момент есть только отдельные работы, в которых затрагивается данный проблемный вопрос [11].

**Изменение 4.**

Дополнена часть 3 статьи 6 Федерального Закона №152 «О персональных данных».

Дополнение касается нормы, которая определяет, что Оператор вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных. Обычно такое «другое лицо» называют обработчиком [12] персональных данных, который может специализироваться на таких услугах, и фактически речь идёт об аутсорсинговых услугах в сфере обработки персональных данных.

«Другое лицо» и ранее было обязано соблюдать конфиденциальность, но закон не обязывал «другое лицо» предоставлять Оператору документы по безопасности своей инфраструктуры.

Теперь «другое лицо» обязано по запросу оператора персональных данных, в том числе до обработки персональных данных, предоставлять документы и иную информацию, подтверждающие принятие мер и соблюдение требований по обеспечению безопасности персональных данных.

Таким образом, вводится обязательство сторонних компаний, оказывающих услуги по обработке персональных данных предоставлять оператору, как заказчику услуг или арендатору инфраструктуры, подтверждающие сведения и документы по безопасности применяемых процессов, технологий и инфраструктуры.

**Изменение 5.**

Дополнена часть 6 статьи 6 Федерального Закона №152 «О персональных данных».

Ранее ответственность (перед субъектом персональных данных) иностранных лиц, занимающихся обработкой персональных данных законом не регламентировалась. Принципиально была указана только ответственность оператора.

Теперь, в случае если оператор поручает обработку персональных данных иностранному физическому лицу или иностранному юридическому лицу, ответственность перед субъектом персональных данных за действия указанных лиц несет и оператор, и лицо, осуществляющее обработку персональных данных по поручению оператора.

Таким образом, вводится совместная ответственность, как самого оператора, так и иностранного обработчика персональных данных.

Рассмотрим данное изменение более подробно. Как уже было отмечено выше, требования Российского законодательства теперь распространяются и на иностранных физических и юридических лиц, занимающихся обработкой персональных данных граждан Российской Федерации. При этом, за исключением отдельных особенных случаев, закон предусматривает обязательность получения согласия на обработку персональных данных от гражданина, и в данном документе обязательно указываются реквизиты организаций или физических лиц, кому будут переданы персональные данные для обработки. Соответственно, субъект персональных данных, изучив перед подписанием содержание согласия, должен быть полностью информирован о местонахождении своих персональных данных. Частным случаем является, когда оператор (работодатель) поручает обработку персональных данных иной организации, по соответствующему соглашению. Однако и в данном случае реквизиты такого обработчика персональных данных указываются в согласии, и субъект является полностью информированным как об операторе, так и обработчике, которому персональные данные будут переданы. В данном случае можно рассматривать обработчика персональных данных как аутсорсера, работающего по соглашению и договору с оператором.

В случае наличия такого аутсорсера, причём независимо от того, является ли он Российским или иностранным физическим или юридическим лицом, между оператором и аутсорсером (обработчиком), должен быть заключён договор на оказание данного вида работ и услуг. Также обязательно указывается конкретный перечень персональных данных, которые могут быть переданы такому обработчику. Сам обработчик при этом обязан предоставить оператору информацию о безопасности своей информационной инфраструктуры.

Дополнительно заметим, что закон устанавливает ключевой принцип, заключающийся в том, что базы с персональными данными граждан Российской Федерации, а также работа с ними (включающая запись, систематизацию, накопление, хранение, уточнение, извлечение данных) должны находиться и осуществляться на территории Российской Федерации[2]. Исходя из этого следует, что иностранные обработчики персональных данных могут физически заниматься данной работой именно на территории Российской Федерации, а, следовательно, доступны для контрольных органов и контрольных мероприятий, и могут быть привлечены к штрафным санкциям за допущенные нарушения.

К иностранным юридическим лицам, собирающим и обрабатывающим персональные данные граждан Российской Федерации, также относятся и компании, хотя и находящиеся за рубежом, но ведущие деятельность в информационной сфере, и предоставляющие электронные сервисы, в том числе, и на территории России посредством сети «Интернет». В настоящее время существует большое множество таких глобальных электронных услуг и сервисов: средства коммуникации, торговые площадки, образовательные ресурсы и т.д. Наиболее вероятным нарушением при этом является размещение баз с персональными данными Российских пользователей на территории другого государства. Однако при этом за пользование сервисами и услугами таковые компании обычно взимают с пользователей плату, в связи с чем иностранные компании такого рода имеют расчётные счета в Российских банках. Поэтому, и к этим компаниям вполне возможно применение штрафных санкций и мер по возмещению ущерба с их локальных счетов на территории Российской Федерации.

**Изменение 6.**

Уточнено требование к согласию субъекта персональных данных на обработку его персональных данных, содержащееся в части 1 статьи 9 Федерального Закона №152 «О персональных данных».

Ранее согласие должно было быть конкретным, информированным и сознательным.

Теперь к этим критериям добавлены ещё два: предметным и однозначным.

Таким образом, следует трактовать два новых понятия о согласии на обработку персональных данных – однозначность понимания данного согласия и его предметность. Что касается предметности, то это понятие говорит о том предмете, в связи с которым данное согласие необходимо. Субъект персональных данных и оператор, как правило, вступают в некие договорные отношения, при этом это конкретная услуга или набор услуг, которые исполнитель оказывает, а заказчик получает. Исходя из этого, следует чётко определить, для целей выполнения каких работ или услуг оператор получает согласие на обработку персональных данных. В свою очередь, это означает необходимость указания конкретных узких целей сбора и обработки персональных данных, взаимоувязанных с конкретными работами или услугами. Выражая предметность согласия, законодатель хоть и не запрещает прямо, но фактически указывает на то, что под каждую отдельную цель,

[2]Исключения есть, но они касаются, прежде всего, задач государственного значения.

работу или услугу, следует формировать соответствующее согласие, и при этом недопустимо получение согласия «в целом», на все виды возможного взаимодействия оператора с субъектом. Наиболее больной точкой, которая послужила толчком для возникновения такой дополнительной формулировки, скорее всего, является неконтролируемая «таргетированная» реклама со стороны компаний, в которые когда-либо обращался субъект персональных данных.

Однозначность согласия – несколько более трудная характеристика, поскольку прямо в законодательстве трактовки данного понятия не приводится. С одной стороны, как и следует из словарного определения[3] самого понятия «однозначности», как единственности, определённости, одновариантности (одного возможного значения), однозначность говорит о недопустимости свободной трактовки формулировок согласия. С другой стороны, под однозначностью согласия можно понимать наличие однозначного волеизъявления с помощью заявления или четкого утвердительного действия, – по аналогии, как это реализовано в международных нормах и правилах[4], в зарубежных странах [13]. Тогда в этом смысле однозначность ещё будет выражаться и в тех действиях, которые совершил субъект, чтобы дать своё согласие (поставил собственноручную подпись, отметил «чекбокс» (флаговая кнопка) в электронной форме и нажал на кнопку «зарегистрироваться» и т.д.). Вся эта совокупность действий должна говорить о том, что, выполняя их, субъект чётко понимает их смысл, содержание и назначение.

**Изменение 7.**

Дополнена статья 11 Федерального Закона №152 «О персональных данных».

Ранее ситуация, когда организация (оператор) требовала от клиента дать согласие на обработку биометрических персональных данных, оставалась не до конца определённой. Хотя при этом, биометрические данные в большинстве случаев не являются необходимыми для установления деловых отношений между Оператором и субъектом (клиентом), выполнения работ и оказания услуг.

Теперь, за исключением отдельных случаев, предоставление биометрических персональных данных не может быть обязательным. Закрепляется, что оператор не вправе отказывать в обслуживании, в случае отказа субъекта персональных данных предоставить биометрические персональные данные и/или дать согласие на обработку персональных данных, если в соответствии с федеральным законом получение оператором согласия на обработку персональных данных не является обязательным.

Таким образом, обособленно разграничивается категория биометрических персональных данных, уязвимость которых может иметь наиболее неблагоприятные последствия. Также однозначно определяется, что требование предоставления биометрических данных должно быть законодательно обосновано.

**Изменение 8.**

Изменён пункт 3 статьи 14 Федерального Закона №152 «О персональных данных».

Изменение касается существующей нормы, которая определяет право субъекта персональных данных на получение информации, касающейся обработки его персональных данных.

[3]Толковый словарь русского языка. URL: https://556.slovaronline.com/58622-ОДНОЗНАЧНЫЙ (дата обращения: 07.09.2022).

[4]Н.Мазурин. Комментарий к поправкам в Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».
URL: https://zakon.ru/blog/2022/08/02/kommentarij_k_popravkam_v_federalnyj_zakon_ot_27072006__152-fz_o_personalnyh_dannyh_n_i_mazurin_ya_e (дата обращения: 07.09.2022).

Ранее не было чёткости в вопросах о том, сразу или не сразу, а также в каком виде должны предоставляться оператором сведения, запрашиваемые субъектом персональных данных.

Теперь установлен конкретный срок – 10 рабочих дней с момента обращения субъекта персональных данных, либо получения от него запроса. В течение этого срока оператор должен рассмотреть запрос или обращение и предоставить субъекту персональных данных необходимые сведения. Предусмотрено также, что оператор может продлить этот срок ещё на 5 дней, направив об этом субъекту персональных данных мотивированное уведомление. Также чётко определяется форма ответа – она должна быть такой же, в которой получен запрос.

Таким образом, снята неопределённость в процедуре получения субъектами персональных данных ответов от соответствующих операторов. На письменный запрос должен быть письменный ответ, на электронный запрос может быть дан электронный ответ, и максимальный срок ответа не может превышать 15 рабочих дней.

**Изменение 9.**

Изменён подпункт 2 пункта 1 статьи 18.1 Федерального Закона №152 «О персональных данных».

Как и ранее, оператор персональных данных обязан создать политику в отношении обработки персональных данных и другие локальные документы.

Однако теперь уточняются требования к составу и содержанию таких локальных нормативно-правовых актов оператора. Принципиально, что теперь становится необходимо определять отдельно для каждой цели обработки персональных данных: категории субъектов персональных данных, перечни персональных данных, способы и сроки обработки и уничтожения персональных данных. Кроме того, процедуры защиты персональных данных и устранения нарушений должны быть также определены локальными документами оператора.

Таким образом, хоть и без установления конкретного перечня, но расширяется спектр локальных нормативно-правовых документов оператора, а также конкретизируется их содержание с задачей недопущения смешивания персональных данных, обрабатываемых в различных целях. Смешивание персональных данных, обрабатываемых в различных целях, не допускалось и ранее. Но именно сейчас установлено, что оператор для пресечения такой возможности обязан разграничить составы персональных данных на самом начальном этапе и задокументировать эти основы.

**Изменение 10.**

Дополнена пунктом 2 статья 18.1 Федерального Закона №152 «О персональных данных».

Дополнение касается существующей нормы о том, что Оператор обязан опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки персональных данных и к сведениям о реализуемых требованиях к защите персональных данных.

Требование об открытости и доступности политики безопасности в отношении обработки персональных данных, было уже давно.

Но теперь внесено довольно важное техническое уточнение, что такая политика должна быть опубликована на каждом сайте, на котором осуществляется сбор персональных данных.

Таким образом, вполне логичная необходимость размещения на сайте документа, определяющего политику обработки персональных данных организацией, которая ранее следовала косвенно, из контекста, теперь закреплена прямым требованием закона.

**Изменение 11.**

Дополнена сразу тремя пунктами 12, 13 и 14 статья 19 Федерального Закона №152 «О персональных данных».

Ранее операторы персональных данных не были обязаны взаимодействовать с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГОССОПКА). В предыдущей редакции закона ГОССОПКА не упоминалась вообще. Взаимодействие с данной системой предусматривалось только для объектов критической информационной инфраструктуры (КИИ) [14, 15], что регламентируется другим законодательством, в частности, Федеральным законом №187 «О безопасности критической информационной инфраструктуры Российской Федерации»[5].

Теперь операторам персональных данных будет необходимо наладить взаимодействие с системой ГОССОПКА и информировать о компьютерных инцидентах, повлекших нарушение режима конфиденциальности обработки персональных данных.

Таким образом, вводится совершенно новая процедура, которую предстоит освоить операторам персональных данных. В настоящий момент ожидается выход соответствующих регламентирующих документов, которые определят порядок взаимодействия операторов с системой ГОССОПКА.

Надо отметить, что в целом, ГОССОПКА – это децентрализованная система, представляющая собой иерархически взаимодействующие государственные и коммерческие центры, которые непрерывно делятся информацией о зафиксированных инцидентах и способах противодействия им.

В настоящее время подключение к инфраструктуре ГОССОПКА возможно двумя способами:

– заключить договор с уже созданным центром ГОССОПКА, оказывающим свои услуги на основании лицензии;

– создать свой корпоративный (ведомственный) сегмент, взаимодействующий с главным центром ГОССОПКА.

Очевидно, для малого бизнеса каждое из решений будет весьма затратным. Организация взаимодействия с системой ГОССОПКА может потребовать внедрения дополнительных программных продуктов, как например Naumen Service Desk, «vsDesk», «1С:ITIL Управление информационными технологиями предприятия ПРОФ» [16]. Практика исполнения данного требования закона должна появиться уже в самое ближайшее время. Есть основания ожидать появления отдельного сервиса (ресурса) для операторов персональных данных, посредством которого они смогут передавать сведения в систему ГОССОПКА.

**Изменение 12.**

Изменена статья 20 Федерального Закона №152 «О персональных данных».

Статья 20 Федерального Закона №152 «О персональных данных» устанавливала регламентные сроки реагирования оператора при обращении к нему субъекта персональных данных либо при получении запроса субъекта персональных данных или его представителя, а также уполномоченного органа по защите прав субъектов персональных данных.

Ранее по большинству обращений оператору отводился срок на подготовку ответа 30 дней. Теперь этот срок снижен до 10 рабочих дней с возможностью мотивированного продления ещё на 5 рабочих дней, т.е. максимально до 15 рабочих дней. Закреплена также

[5]URL: http://www.kremlin.ru/acts/bank/42128 (дата обращения: 07.09.2022).

в виде самостоятельной процедуры возможность обращения субъекта с требованием о прекращении обработки персональных данных (табл. 1).

Таким образом, срок ответов по всем штатным вопросам и обращениям снижается с 30 дней до максимум 15 рабочих дней.

*Таблица 1. Сроки реагирования оператора на обращения*

| Источник обращения | Повод обращения | Срок рассмотрения | |
|---|---|---|---|
| | | Было (до 01.09.2022) | Стало (с 01.09.2022) |
| Субъект | Ознакомление со своими персональными данными | 30 дней | 10 рабочих дней (+ 5 дней продление) |
| Субъект | Мотивированный отказ в предоставлении сведений | 30 дней | 10 рабочих дней (+ 5 дней продление) |
| Уполномоченный орган | Запрос | 30 дней | 10 рабочих дней (+ 5 дней продление) |
| Субъект | Требование прекратить обработку | Не определялось | 10 рабочих дней (+ 5 дней продление) |

**Изменение 13.**

Дополнена пунктом $3^1$ статья 21 Федерального Закона №152 «О персональных данных».

Ранее оператор не был обязан сообщать о произошедших инцидентах, нарушивших безопасность персональных данных.

Теперь вводится новая процедура, предусматривающая обязательное уведомление уполномоченного органа по защите персональных данных, как о самих произошедших инцидентах, так и о результатах их внутреннего расследования. Кроме того, установлены очень жёсткие сроки для этого:

– 24 часа отводится на информирование о факте возникшего инцидента;

– 72 часа отводится на информирование о результатах проведённой внутренней проверки и расследования.

Таким образом, оператор персональных данных должен заранее проработать регламент действий на случай возникновения инцидентов, а также определить сотрудников, на которых будут возлагаться функции по расследованию. Сами расследования должны будут проводиться крайне оперативно в считанные часы.

Форма уведомления об инцидентах, а также о результатах их расследования, заполняется и отправляется в электронном виде с официального сайта уполномоченного органа по защите персональных данных[6]. Для этого требуется учётная запись на портале государственных услуг, привязанная к организации – оператору персональных данных.

**Изменение 14.**

Сокращены основания, по которым оператор может осуществлять обработку персональных данных без обязательного уведомления уполномоченного органа, которые изложены в статье 22 Федерального Закона №152 «О персональных данных».

До настоящего времени было 9 оснований, освобождающих оператора от обязанности подавать уведомление и, соответственно, вступать в реестр операторов персональных данных.

Теперь из 9 оснований остаются в силе только три:

[6]Портал государственных услуг. Форма подачи сведений об инциденте безопасности. URL: https://esia2.rkn.gov.ru/auth/pdincidentform (дата обращения: 07.09.2022).

– при обработке персональных данных включенных в государственные информационные системы персональных данных, созданные в целях защиты безопасности государства и общественного порядка;

– при обработке персональных данных исключительно без использования средств автоматизации;

– при обработке персональных данных, обрабатываемых в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности.

Особенно отметим, что такие наиболее частые основания, позволявшие операторам заниматься обработкой персональных данных без обязательного включения в реестр, как обработка персональных данных своих собственных сотрудников и обработка персональных данных клиента с целью исполнения договорных обязательств – теперь из перечня исключены.

Таким образом, практически любая организация теперь обязана подавать уведомление и вступать в реестр операторов персональных данных. Для рядовой коммерческой компании малого бизнеса, деятельность которых ориентировано на сектор массового потребления товаров или услуг, и не связанных ни с государственными информационными системами, ни с транспортной безопасностью, единственным основанием, чтобы не вступать в реестр, фактически остаётся переход на неавтоматизированную обработку персональных данных.

Полноценная реализация существенно изменившихся требований законодательства подразумевает повышение квалификации специалистов, занимающихся защитой персональных данных в организациях [17] с учётом особенностей интенсивно развивающейся цифровой среды [18].

## Заключение

Проведённый анализ показывает, что с 1 сентября 2022 г. в силу вступают 14 принципиальных изменений и дополнений в требования по обработке персональных данных. Ряд из них – критический, требующий проведения в организации комплекса работ по внедрению новых процессов, дополнительному назначению новых ответственных сотрудников, выделению финансовых средств на реализацию.

Все нововведения можно условно разделить на:

– ограничительные, заключающиеся в запрете некоторых ранее допустимых действий, а также необходимости ужесточения внутренних организационных процессов и разработки дополнительных локальных документов, либо переработки существующих, в том числе касающихся договорных отношений компании с партнёрами;

– активные, заключающиеся в необходимости создания новых процессов, привлечения новых специалистов и внедрения новых систем.

К ограничительным нововведениям можно отнести:

– запрет вносить ряд условий в договорные отношения с клиентами;

– недопустимость игнорировать недостатки в безопасности инфраструктуры компаний-партнёров;

– недопустимость применения и оформления абстрагированных «многофункциональных» согласий на обработку персональных данных;

– прямой запрет на принудительный сбор биометрических персональных данных;

– снижение сроков реагирования на обращения субъектов персональных данных;

– установление формы ответа на обращения субъектов персональных данных;

– обязательство определять состав персональных данных и методы их обработки отдельно для каждой из целей;

– прямое указание на публикацию политики обработки персональных данных непосредственно на том электронном ресурсе, где осуществляется их сбор.

К активным нововведениям можно отнести:

– необходимость организовать взаимодействие с системой ГОССОПКА;

– обязательное (и фактически – немедленное) информирование уполномоченного органа о возникших инцидентах, нарушивших безопасность персональных данных;

– обязательное проведение внутренних расследований инцидентов и предоставление уполномоченному органу отчёта по результатам расследований;

– обязательная подача уведомления и вступление в реестр операторов персональных данных, если только обработка не проводится исключительно неавтоматизированными методами.

Первоочередными задачами для любой организации на текущий момент являются:

– назначение ответственного сотрудника за взаимодействие с системой ГОССОПКА и системой информирования об инцидентах;

– разработка регламента реагирования на возникшие инциденты с соответствующим информированием (обучением) всех сотрудников, которые, так или иначе, участвуют в процессах, связанных с обработкой персональных данных, имеют доступ к информационным системам, инфраструктуре компании;

– подготовка и формирование группы сотрудников, которые составят комиссию по расследованию инцидентов;

– доработка локальных документов, приведя их в соответствие новым ограничительным требованиям;

– проведение обучения сотрудников организации с учётом изменений законодательства и изменений во внутренних процессах организации.

Взаимодействие с системой ГОССОПКА, равно как и обнаружение и расследование инцидентов безопасности, фактически диктуют требования по выстраиванию в организации системы управления инцидентами информационной безопасности, выделения на это дополнительного финансирования, и внедрения сопутствующего программного обеспечения.

Автор данной статьи является разработчиком и спикером программы повышения квалификации «Защита персональных данных в организации», проводимой Институтом цифровых компетенций Финансового Университета при Правительстве РФ. Данная программа учитывает все текущие изменения в законодательстве и направлена на формирование у слушателей соответствующих знаний и компетенций. Также следует отметить, что одной из наиболее актуальных задач в настоящий период является не только подготовка специалистов по защите персональных данных, владеющих организационно-управленческим и аналитическим мышлением, но также и донесение знаний и пониманий важности осмысленного отношения к своим персональным данным до широких слоёв граждан, формирование культуры обращения с персональными данными и обеспечения персональной безопасности личности в информационной среде.

Кроме рассмотренных, есть ещё ряд не затронутых в данной статье нововведений и изменений, которые вступят в силу с 1 марта 2023 г. По ним автором планируется провести отдельный анализ.

СПИСОК ЛИТЕРАТУРЫ:

1. Иванова А.П. Утечка персональных данных: большая проблема в цифровую эпоху. Социальные и гуманитарные науки. Отечественная и зарубежная литература. Серия 4: Государство и право. 2020, № 4, с. 100–107. URL: https://www.elibrary.ru/item.asp?id=44205398 (дата обращения: 07.09.2022). – EDN XLOSRY.
2. Тесленко И.Б., Дилигина О.Б., Муравьева Н.В., Абдуллаев Н.В. Развитие экосистемы цифровой экономики в России. Экономика и предпринимательство. 2018, № 9(38), с. 150–154. URL: https://www.elibrary.ru/item.asp?id=36854678 (дата обращения: 07.09.2022). – EDN YVFAAX.
3. Сиротский А.А. Информационные и методические проблемы информационной безопасности личности в современном деловом обороте. «Системы безопасности – 2015». Материалы 24-й международной научно-технической конференции (26 ноября 2015 г., Москва). М.: Академия ГПС МЧС России. 2015, с. 104–107. URL: https://www.elibrary.ru/item.asp?id=24867328 (дата обращения: 07.09.2022). – EDN UYELWX.
4. Балаев Р.С. Факторы рисков и угроз экзистенциальной безопасности личности в информационном обществе. Наука XXI века: новый подход. Материалы XIV молодёжной международной научно-практической конференции студентов, аспирантов и молодых учёных. Научно-издательский центр «Открытие». 2015, с. 56–63. URL: https://www.elibrary.ru/item.asp?id=24572966 (дата обращения: 07.09.2022). – EDN URSZKT.
5. Колоткина О.А. К вопросу о соотношении понятий «безопасность личности» и «личная безопасность». Novainfo.Ru. 2016, с. 374–378. URL: https://www.elibrary.ru/item.asp?id=27543875 (дата обращения: 07.09.2022). – EDN XETHUB.
6. Сиротский Алексей А., Резниченко Сергей А. Формализованная модель аудита информационной безопасности организации на предмет соответствия требованиям стандартов. Безопасность информационных технологий, [S.l.], т. 28, № 3, с. 103–117, 2021. DOI: http://dx.doi.org/10.26583/bit.2021.3.09. URL: https://www.elibrary.ru/item.asp?id=46709372 (дата обращения: 07.09.2022). – EDN LSDPLE.
7. Сиротский А.А. Информационная безопасность личности и защита персональных данных в современной коммуникативной среде. Технологии техносферной безопасности. Научный интернет-журнал. 2013, Вып. 4(50), с. 3–10. URL: https://www.elibrary.ru/item.asp?id=21482445 (дата обращения: 07.09.2022). – EDN SCCPQV.
8. Гнедков А.В., Нищик А.В. Особенности распространения персональных данных в последней редакции законодательства о персональных данных. Научно-методическое обеспечение оценки качества образования. 2022, № 1(15), с. 49–52. URL: https://www.elibrary.ru/item.asp?id=48657880 (дата обращения: 07.09.2022). – EDN DTSTJD.
9. Абрамова А.Г. Современные проблемы осуществления защиты персональных данных в сети: Основополагающие принципы защиты персональных данных. Регион и мир. 2020, т. 11, № 4, с. 21–25. URL: https://www.elibrary.ru/item.asp?id=44023034 (дата обращения: 07.09.2022). – EDN EVEAYH.
10. Воробьев Е.Г. Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных. Учебное пособие. СПб.: ООО «Издательский центр «Интермедия», 2016. – 432 с. URL: https://www.elibrary.ru/item.asp?id=38309216 (дата обращения: 07.09.2022). – EDN ELGJNP.
11. Александрова В.И. Особенности обработки персональных данных несовершеннолетних в информационных системах персональных данных. Молодой ученый. 2016, № 19(123), с. 40–42. URL: https://www.elibrary.ru/item.asp?id=26740293 (дата обращения: 07.09.2022). – EDN WNECMB.
12. Грибанов А.А. Определение персональных данных, разграничение операторов и обработчиков персональных данных. Судья. 2021, № 4(124), с. 30–34. URL: https://www.elibrary.ru/item.asp?id=46200393 (дата обращения: 07.09.2022). – EDN GRQPCH.
13. Денискина В.Г., Курдявка К.Е. Правовое регулирование персональных данных в РФ И ФРГ. Теория и практика Германистов: состояние и перспективы. Сборник статей. VIII Межвузовская междисциплинарная конференция преподавателей и студентов. Издательство: Всероссийская академия внешней торговли Министерства экономического развития РФ. Москва. 2020, с. 89–94. URL: https://www.elibrary.ru/item.asp?id=47142064 (дата обращения: 07.09.2022). – EDN GUAHIY.
14. Наталичев Роман В. и др. Эволюция и парадоксы нормативной базы обеспечения безопасности объектов критической информационной инфраструктуры. Безопасность информационных технологий, [S.l.], т. 28, № 3, с. 6–27, 2021. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2021.3.01. URL: https://www.elibrary.ru/item.asp?id=46709364 (дата обращения: 07.09.2022). – EDN JIMDXU.
15. Вавичкин Александр Н. и др. К вопросу категорирования объектов критической информационной инфраструктуры высших учебных заведений. Безопасность информационных технологий, [S.l.], т. 26,

№ 2, с. 44–57, 2019. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2019.2.03. URL: https://www.elibrary.ru/item.asp?id=38568103 (дата обращения: 07.09.2022). – EDN TMBXWG.

16. Красножон Ю.Г. Процесс управления инцидентами информационной безопасности в центрах обработки данных ФНС России. Стратегии социально-экономического развития северного региона Крыма на долгосрочный период. Материалы I Межрегиональной научно-практической конференции. Армянск, 2018, с. 69–74. URL: https://www.elibrary.ru/item.asp?id=34932009 (дата обращения: 07.09.2022). – EDN XNNWOL.
17. Сиротский А.А. Опыт участия в программе «Персональные цифровые сертификаты 2020» в качестве разработчика и преподавателя курса по защите персональных данных. Преподавание информационных технологий в Российской Федерации. Сборник научных трудов Девятнадцатой открытой Всероссийской конференции. Москва, онлайн, 19-20 мая 2021. М.: ООО «1С-Паблишинг». 2021, с. 323–325. URL: https://www.elibrary.ru/item.asp?id=47218009 (дата обращения: 07.09.2022). – EDN CXRQDB.
18. Малюк Анатолий А., Малюк Зоя П. Актуальные вопросы создания системы массового обучения культуре информационной безопасности. Безопасность информационных технологий, [S.l.], т. 28, № 4, с. 6–21, 2021. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2021.4.01. URL: https://www.elibrary.ru/item.asp?id=47422956 (дата обращения: 07.09.2022). – EDN XHPGMY.

REFERENCES:

[1] Ivanova A.P. Personal data leakage: a big problem in the digital age. Social and humanities. Domestic and foreign literature. Series 4: State and Law. 2020, no. 4, p. 100–107. URL: https://www.elibrary.ru/item.asp?id=44205398 (accessed: 07.09.2022) (in Russian). – EDN XLOSRY.
[2] Teslenko I.B., Diligina O.B., Muravyeva N.V., Abdullaev N.V. Development of the digital economy ecosystem in Russia. Economics and entrepreneurship. 2018, no. 9(38), p. 150–154. URL: https://www.elibrary.ru/item.asp?id=36854678 (accessed: 07.09.2022) (in Russian). – EDN YVFAAX.
[3] Sirotskiy A.A. Information and methodological problems of personal information security in modern business turnover."Security Systems – 2015". Proceedings of the 24th International Scientific and Technical Conference (November 26, 2015, Moscow). M.: Academy of the State Fire Service of the Ministry of Emergencies of Russia. 2015, p. 104–107. URL: https://www.elibrary.ru/item.asp?id=24867328 (accessed: 07.09.2022) (in Russian). – EDN UYELWX.
[4] Balaev R.S. Factors of risks and threats to existential security of the individual in the information society. Science of the XXI century: a new approach. Materials of the XIV youth international scientific and practical conference of students, graduate students and young scientists. Otkritie Research and Publishing Center. 2015, p. 56–63. URL: https://www.elibrary.ru/item.asp?id=24572966 (accessed: 07.09.2022) (in Russian). – EDN URSZKT.
[5] Kolotkina A.A. To the question of the relationship between the concepts of "personal security" and "personal security". Novainfo.Ru. 2016, p. 374–378. URL: https://www.elibrary.ru/item.asp?id=27543875 (accessed: 07.09.2022) (in Russian). – EDN XETHUB.
[6] Sirotskiy Alexei A., Reznichenko Sergei A. A formalized model of an organization information security audit for compliance with the requirements of standards. IT Security (Russia), [S.l.], v. 28, no. 3, p. 103–117, 2021. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2021.3.09. URL: https://www.elibrary.ru/item.asp?id=46709372 (accessed: 07.09.2022) (in Russian). – EDN LSDPLE.
[7] Sirotskiy A.A. Personal Information Security and Personal Data Protection in the Modern Communication Environment. Technosphere Security Technologies. Scientific online journal. 2013, Issue 4 (50), p. 3-10. URL: https://www.elibrary.ru/item.asp?id=21482445 (accessed: 07.09.2022) (in Russian). – EDN SCCPQV.
[8] Gnedkov A.V., Nischik A.V. Features of the distribution of personal data in the latest version of the legislation on personal data. Scientific and methodological assurance of the assessment of the quality of education. 2022, no. 1(15), p. 49–52. URL: https://www.elibrary.ru/item.asp?id=48657880 (accessed: 07.09.2022) (in Russian). – EDN DTSTJD.
[9] Abramova A.G. Current problems of personal data protection in the network: Fundamental principles of personal data protection. Region and world. 2020, vol. 11, no. 4, p. 21–25. URL: https://www.elibrary.ru/item.asp?id=44023034 (accessed: 07.09.2022) (in Russian). – EDN EVEAYH.
[10] Vorobyev E.G. Ensuring the security of personal data during its processing in personal data information systems. Tutorial. St. Petersburg: Intermedia Publishing Center LLC, 2016. – 432 p. URL: https://www.elibrary.ru/item.asp?id=38309216 (accessed: 07.09.2022) (in Russian). – EDN ELGJNP.
[11] Alexandrova V.I. Features of processing personal data of minors in personal data information systems. Young scientist. 2016, no. 19(123), p. 40–42. URL: https://www.elibrary.ru/item.asp?id=26740293 (accessed: 07.09.2022) (in Russian) – EDN WNECMB.

[12] Gribanov A.A. Definition of personal data, delimitation of operators and processors of personal data. Judge. 2021, no. 4(124), p. 30–34. URL: https://www.elibrary.ru/item.asp?id=46200393 (accessed: 07.09.2022) (in Russian). – EDN GRQPCH.

[13] Deniskina V.G., Kurdiavka K.E. Legal regulation of personal data in the Russian Federation and Germany. Theory and practice of Germanists: state and prospects. Collection of articles. VIII Intercollegiate Interdisciplinary Conference of Faculty and Students. Publishing house: All-Russian Academy of Foreign Trade of the Ministry of Economic Development of the Russian Federation. Moscow. 2020, p. 89–94. URL: https://www.elibrary.ru/item.asp?id=47142064 (accessed: 07.09.2022) (in Russian). – EDN GUAHIY.

[14] Natalichev Roman V. et al. Evolution and paradoxes of the regulatory framework for ensuring the security of critical information infrastructure facilities. IT Security (Russia), [S.l.], v. 28, no. 3, p. 6–27, 2021. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2021.3.01. URL: https://www.elibrary.ru/item.asp?id=46709364 (accessed: 07.09.2022) (in Russian). – EDN JIMDXU.

[15] Vavichkin Alexander N. et al. To the issue of categorization of critical informational infrastructure objects in higher education. IT Security (Russia), [S.l.], v. 26, no. 2, p. 44–57, 2019. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2019.2.03. URL: https://www.elibrary.ru/item.asp?id=38568103 (accessed: 07.09.2022) (in Russian). – EDN TMBXWG.

[16] Krasnozhon Yu.G. The process of managing information security incidents in the data processing centers of the Federal Tax Service of Russia. Strategies for the socio-economic development of the northern region of Crimea for the long term. Materials of the I Interregional Scientific and Practical Conference. Armyansk, 2018, p. 69–74. URL: https://www.elibrary.ru/item.asp?id=34932009 (accessed: 07.09.2022) (in Russian). – EDN XNNWOL.

[17] Sirotskiy A.A. Experience of participation in the Personal Digital Certificates 2020 program as a developer and teacher of a course on personal data protection. Teaching information technologies in the Russian Federation. Collection of scientific works of the Nineteenth Open All-Russian Conference. Moscow, online, May 19-20, 2021. M.: LLC "1C-Publishing." 2021, p. 323–325. URL: https://www.elibrary.ru/item.asp?id=47218009 (accessed: 07.09.2022) (in Russian). – EDN CXRQDB.

[18] Malyuk Anatoly A., Malyuk Zoya P. Topical issues of creating a mass education system for information security culture. IT Security (Russia), [S.l.], v. 28, no. 4, p. 6–21. 2021. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2021.4.01. URL: https://www.elibrary.ru/item.asp?id=47422956 (accessed: 07.09.2022) (in Russian). – EDN XHPGMY.

*Поступила в редакцию – 14 сентября 2022 г. Окончательный вариант – 08 ноября 2022 г.*
*Received – September 14,2022. The final version – November 08, 2022.*