**Александр Чумаченко,** старший юрист

# 10 вопросов юристу по защите персональных данных

Защита персональных данных является важным вопросом не только для тех лиц, к которым персональные данные относятся, но и для лиц, собирающих и обрабатывающих эти данные. В Казахстане с момента принятия профильного закона (Закон о персональных данных) актуальность данного вопроса постоянно увеличивается, в том числе в связи с добавлением законодателем новых требований и уточнением уже действующих. Ниже приводится информация касательно основных аспектов сбора, обработки и защиты персональных данных, на которые следует обратить внимание.



## 1. Какие сведения являются персональными данными?

Под персональными данными понимаются сведения, относящиеся к определенному или определяемому на их основании субъекту персональных данных (**"субъект"**), зафиксированные на электронном, бумажном или ином материальном носителе.

Приведенное определение сформулировано законодателем очень широко. При этом исчерпывающий перечень данных, являющихся персональными, законодательством не установлен. Поэтому заинтересованными лицами (в частности, субъектами и

уполномоченными органами) в качестве персональных данных могут рассматриваться фактически любые сведения, относящиеся к субъекту.

На практике к персональным данным относятся фамилия, имя, отчество, адрес проживания, гражданство, дата рождения, образование, семейное положение, биометрические данные и другие сведения о субъекте. Субъектами являются только физические лица.

## 2. Какие персональные данные можно собирать и обрабатывать?

Персональные данные подразделяются на общедоступные и данные ограниченного доступа. Общедоступными являются те персональные данные, в отношении которых с согласия субъекта установлен свободный доступ (например, для использования в биографических справочниках, телефонных, адресных книгах, общедоступных электронных информационных ресурсах, средствах массовой информации) либо на которые, в соответствии с законодательством Казахстана, не распространяются требования о соблюдении конфиденциальности (например, гласность при рассмотрении судом уголовных дел). Соответственно, все остальные персональные данные по умолчанию являются данными ограниченного доступа. Кроме того, некоторые данные (например, дактилоскопическая и геномная информация) прямо отнесены законодательством к персональным данным ограниченного доступа.

По общему правилу сбор и обработка персональных данных осуществляются с согласия субъекта (его законного представителя) на осуществление таких действий (**"согласие"**). Согласие на требуется, как отмечено выше, если персональные данные находятся в общем доступе на законных основаниях и на них не распространяются требования о конфиденциальности, а также в случаях, определенных законодательством (в частности, ст. 9 Закона о персональных данных). К последним в основном относятся случаи обработки персональных данных государственными органами.

Предварительно сбору и обработке персональных данных лица, осуществляющие данные действия, обязаны определить (и утвердить) перечень персональных данных, необходимых для работы (функционирования) этих лиц, а также законные цели и задачи, преследуемые при сборе и обработке персональных данных. Сбор и обработка персональных данных, по объему и содержанию выходящих за рамки указанного перечня и (или) предоставленного субъектом согласия, а также не соответствующих заявленным целям и задачам сбора и обработки, запрещены.

Таким образом, сбор и обработка допускаются в отношении персональных данных, которые находятся на законном основании в общедоступных источниках (в этом случае собираемые данные должны сопровождаться ссылкой на источник информации), и персональных данных, перечисленных в согласии.

Следует иметь в виду, что положения Закона о персональных данных не распространяются на сбор и обработку персональных данных исключительно для личных и семейных нужд, если при этом не нарушаются права других физических и (или) юридических лиц и требования законодательства Казахстана.

## 3. Кто вправе собирать и обрабатывать персональные данные?

В рамках сбора, обработки и защиты персональных данных законодательство Казахстана о персональных данных оперирует следующими тремя понятиями лиц, которые осуществляют такие действия:

- оператор базы, содержащей персональные данные (**"оператор"**), под которым понимаются государственный орган, физическое и (или) юридическое лицо, осуществляющие сбор, обработку и защиту персональных данных;
- собственник базы, содержащей персональные данные (**"собственник"**), под которым понимаются государственный орган, физическое и (или) юридическое лицо, реализующие в соответствии с законами Республики Казахстан право владения, пользования и распоряжения базой, содержащей персональные данные (**"база"**);
- третье лицо – лицо, не являющееся субъектом, собственником и (или) оператором, но связанное с ними (ним) обстоятельствами или правоотношениями по сбору, обработке и защите персональных данных.

Таким образом, сбор и обработку персональных данных осуществляют, в первую очередь, операторы, а во вторую – третьи лица. Статус собственника, хотя и наделяет соответствующее лицо правами и обязанностями, в целом идентичными правам и обязанностям оператора, предполагает исключительно владение базой, т.е. собственник может и не осуществлять действий по сбору и обработке персональных данных, ограничиваясь только владением базой. Примером такой ситуации является предоставление услуг облачного хранения данных. При осуществлении сбора и обработки персональных данных собственник приобретает статус оператора.

Следует иметь в виду, что определение того, кем (оператором или третьим лицом) выступает лицо при сборе и обработке персональных данных, имеет важное значение, поскольку требования законодательства о персональных данных к операторам и третьим лицам отличаются. Например, наименование (ФИО) и БИН (ИИН) оператора должны быть включены в согласие субъекта, а в отношении третьих лиц такая информация не требуется. Соответственно, в случае если лицо, собирающее и обрабатывающее персональные данные, будет признано не третьим лицом, а оператором и при этом оно не будет включено в согласие субъекта, действия этого лица по сбору и обработке персональных данных могут быть признаны незаконными.

Обозначенные выше понятия оператора и третьего лица, установленные законодателем, не позволяют в полной мере их разграничить. Понятие оператора сформулировано очень широко и фактически позволяет относить к операторам любое лицо, которое собирает и обрабатывает персональные данные. То есть лица, которые обрабатывают персональные данные в рамках правоотношений (например, договорных обязательств) с оператором, тоже подпадают под определение оператора. При этом неясен предмет правоотношений между оператором и его контрагентом для целей отнесения последнего к третьим лицам, а именно должны ли правоотношения быть направлены исключительно на обработку персональных

данных или же обработка персональных данных может не быть основным предметом правоотношений сторон и только сопутствовать их реализации.

Отсутствие надлежащего правового регулирования и однозначных, вразумительных разъяснений уполномоченных органов по этому вопросу влечет риск нарушения требований законодательства и привлечения к ответственности лиц, собирающих и обрабатывающих персональные данные.

## 4. Какие требования установлены в отношении согласия субъекта?

Как было отмечено выше, сбор и обработка персональных данных осуществляются с согласия субъекта или его законного представителя, кроме случаев, предусмотренных законодательством. Сбор и обработка (включая использование) персональных данных должны осуществляться только в рамках и в целях достижения оператором заранее определенных законных целей. Кроме того, оператором должен быть разработан и утвержден перечень персональных данных, необходимый и достаточный для выполнения осуществляемых им задач, и такой перечень должен быть закрытым (исчерпывающим).

Помимо иной информации на усмотрение оператора, согласие должно содержать:

- данные об операторе – ФИО и ИИН физического лица либо наименование и БИН юридического лица;
- ФИО субъекта;
- срок действия согласия;
- перечень собираемых персональных данных;
- указание на то, будет ли оператор трансгранично (за пределы Казахстана) передавать персональные данные в процессе их обработки, а также прямое и недвусмысленное разрешение субъекта на трансграничную передачу;
- указание на то, будет ли оператор передавать персональные данные третьим лицам, а также прямое и недвусмысленное разрешение субъекта на передачу персональных данных третьим лицам;
- указание на то, будет ли оператор распространять собранные персональные данные в общедоступных источниках, а также прямое и недвусмысленное разрешение субъекта на распространение персональных данных в общедоступных источниках.

Согласие должно быть дано субъектом или его законным представителем письменно, в форме электронного документа, посредством государственного (негосударственного) сервиса контроля доступа к персональным данным либо иным способом с применением элементов защитных действий (электронно-цифровой подписи), не противоречащих законодательству Казахстана. При этом, несмотря на активное развитие в Казахстане цифровизации и электронного документооборота, на настоящий момент наиболее надежным (безопасным для оператора) и универсальным способом получения согласия является его составление в простой

письменной форме за собственноручной подписью субъекта (его законного представителя).

Это связано с тем, что бремя доказывания правомерности действий оператора по сбору и обработке персональных данных лежит на операторе (любые сомнения в правомерности действий оператора толкуются в пользу субъекта), а за нарушение законодательства о персональных данных предусмотрена строгая ответственность. Кроме того, электронные цифровые подписи физических лиц применяются только в ограниченном круге сервисов, в частности, при получении государственных услуг на портале "электронного правительства" и других государственных сервисах, т.е. на практике физические лица пока не могут получить универсальную электронную цифровую подпись, которой они могли бы подписать согласие в электронной форме.

## 5. Где следует хранить персональные данные?

Персональные данные подлежат хранению в базах. Под базой в Законе о персональных данных понимается совокупность упорядоченных персональных данных. При этом законодатель не уточняет какие-либо конкретные виды и (или) признаки баз, а также механизм их определения. Поэтому оператор вправе самостоятельно определить, что считать и использовать в качестве базы (например, кабинет, полку, шкаф, персональный компьютер), а также в каком количестве и где (в пределах Казахстана) их размещать.

Поскольку из законодательства не следует иное, создание собственного локального сервера (и/или наличие собственного помещения в Казахстане в отношении документов на бумажном носителе) для обработки персональных данных не требуется, поэтому любая компания может передать данную функцию на "аутсорс", при условии соблюдения требований по защите персональных данных, включая обеспечение конфиденциальности персональных данных и наличие согласия субъекта, покрывающего лиц, которые будут фактически осуществлять такую обработку.

Все базы, в которых осуществляется хранение персональных данных, должны быть размещены на территории Казахстана. Данное требование распространяется на документы, содержащие персональные данные, как на бумажном носителе, так и в электронной форме (соответственно, оборудование, на котором хранятся электронные документы с персональными данными, должно быть физически размещено в Казахстане). При этом государственные органы в своих разъяснениях допускают возможность так называемого параллельного хранения персональных данных, в рамках которого персональные данные изначально собираются и обрабатываются (хранятся) в базах на территории Казахстана, после чего происходит их дублирование (при условии наличия согласия субъекта на их трансграничную передачу) в базы за пределами Казахстана.

## 6. Как осуществляется передача персональных данных за пределы Казахстана?

Законодательство Казахстана допускает передачу персональных данных за его пределы (трансграничная передача). По общему правилу трансграничная передача

персональных данных осуществляется только в случае обеспечения соответствующими государствами защиты персональных данных. Если защита персональных данных такими государствами не обеспечивается, трансграничная передача осуществляется в случаях:

- наличия согласия субъекта или его законного представителя на трансграничную передачу персональных данных;
- предусмотренных международными договорами, ратифицированными Казахстаном;
- предусмотренных законами Казахстана, если это необходимо в целях защиты конституционного строя, охраны общественного порядка, прав и свобод человека и гражданина, здоровья и нравственности населения;
- защиты конституционных прав и свобод человека и гражданина, если получение согласия субъекта или его законного представителя невозможно.

Хотя Закон о персональных данных не уточняет этого, трансграничная передача персональных данных подразумевает их переход из одной юрисдикции в другую и, соответственно, изменение законодательства, применимого к обработке персональных данных, с законодательства Казахстана на законодательство государства получателя персональных данных, т.е. после того, как персональные данные будут надлежащим образом трансгранично переданы в базу, находящуюся за пределами Казахстана, к собственнику и операторам этой базы перейдет обязанность обеспечивать защиту персональных данных уже в соответствии с законодательством иностранного государства, на территории которого находится база.

Из Закона о персональных данных неясно, требуется ли для возникновения факта трансграничной передачи персональных данных их передача другому лицу, или же достаточно переместить персональные данные из базы на территории Казахстана в базу, расположенную в иностранном государстве, в рамках одного собственника и (или) оператора. Поэтому при перемещении персональных данных одним и тем же собственником или оператором между своими базами, расположенными в Казахстане и за его пределами (например, между казахстанским структурным подразделением иностранной компании и ее головным офисом за пределами Казахстана или между казахстанской дочерней компанией и ее материнской иностранной компанией), потенциально возникает риск нарушения требования о размещении баз на территории Казахстана.

## 7. Какие требования установлены в отношении защиты персональных данных?

Одним из основных требований для осуществления сбора и обработки персональных данных является обеспечение их защиты. Собственник, оператор и третье лицо обязаны принимать меры (в том числе правовые, организационные и технические) по защите персональных данных, обеспечивающие:

- предотвращение несанкционированного доступа к персональным данным;

- своевременное обнаружение фактов несанкционированного доступа к персональным данным, если такой несанкционированный доступ не удалось предотвратить;
- снижение и по возможности нивелирование неблагоприятных последствий несанкционированного доступа к персональным данным;
- предоставление государственной технической службе доступа к объектам информатизации (электронным информационным ресурсам, программному обеспечению, интернет-ресурсам и информационно-коммуникационной инфраструктуре), посредством которых осуществляется обработка персональных данных, для осуществления обследования обеспечения защищенности процессов хранения, обработки и распространения персональных данных;
- регистрацию и учет сроков действия полученных согласий, случаев передачи персональных данных третьим лицам, их трансграничной передачи и распространения в общедоступных источниках.

Помимо прочего, в целях защиты персональных данных указанные лица обязаны:

- определять перечень лиц, имеющих доступ к персональным данным;
- оповещать уполномоченный орган в сфере защиты персональных данных о случаях незаконного доступа к персональным данным;
- обеспечивать установку средств защиты информации, обновлений программного обеспечения на технических средствах, осуществляющих обработку персональных данных;
- обеспечивать ведение журнала событий систем управления базами;
- обеспечивать ведение журнала действий пользователей, имеющих доступ к персональным данным;
- применять средства контроля целостности персональных данных;
- обеспечивать передачу персональных данных иным лицам (при наличии согласия субъекта, если иное не предусмотрено законодательством Казахстана) по защищенным каналам связи или с применением шифрования;
- выделять бизнес-процессы, связанные со сбором и обработкой персональных данных;
- обеспечивать применение средств криптографической защиты информации для надежного хранения персональных данных;
- применять средства идентификации или аутентификации пользователей при работе с персональными данными.

Оператор, являющийся юридическим лицом, обязан назначить лицо, ответственное за организацию обработки персональных данных, с возложением на него следующих обязанностей:

- осуществление внутреннего контроля за соблюдением оператором и его работниками законодательства Казахстана о персональных данных и их защите, в том числе требований к защите персональных данных;
- доведение до сведения работников оператора положений законодательства Казахстана о персональных данных и их защите по вопросам обработки персональных данных, требований к защите персональных данных;
- осуществление контроля за приемом и обработкой обращений субъектов или их законных представителей.

## 8. Какие документы по персональным данным должны быть разработаны в организации?

Основными документами, которые следует разработать и утвердить в каждой организации в целях осуществления сбора и обработки персональных данных, являются:

- документ, определяющий политику оператора в отношении сбора, обработки и защиты персональных данных (акт работодателя, например, в форме положения или инструкции);
- перечень персональных данных, необходимый и достаточный для выполнения осуществляемых организацией задач (документ, в котором будут определены конкретные цели и задачи сбора и обработки персональных данных, а также конкретный список персональных данных под каждую цель и задачу, например, фамилия, имя, отчество, сведения о социальном и налоговом статусе и прочее для работников организации, либо фамилия, имя, отчество, сведения о налоговом статусе, сведения об осуществлении предпринимательской деятельности и прочее для контрагента);
- перечень лиц (работников), имеющих доступ к персональным данным и осуществляющих их сбор и обработку от лица организации (документ, который будет включать список конкретных работников, обладающих правами на сбор и обработку персональных данных, а также доступа к персональным данным в объеме выполняемых ими трудовых функций, плюс описание их основных обязанностей по обеспечению режима конфиденциальности персональных данных);
- типовая форма согласия, которую будут подписывать субъекты в целях предоставления персональных данных организации;
- типовые положения о соблюдении требований по защите персональных данных для включения в договоры с контрагентами-юридическими лицами;

- акт работодателя (например, в форме приказа) об утверждении указанных выше документов и назначении лица, ответственного за организацию обработки персональных данных в компании.

Дополнительно может потребоваться разработка и других документов в целях исполнения требований законодательства (например, различных журналов учета и регистрации) и (или) исходя из специфики деятельности, осуществляемой организацией (например, отдельных форм согласия для разных категорий субъектов – работников, клиентов, контрагентов и пр.).

В частности, с 2022 года собственники, операторы и третьи лица обязаны осуществлять регистрацию и учет:

- сроков действия полученных согласий;
- случаев передачи персональных данных третьим лицам;
- случаев трансграничной передачи персональных данных;
- случаев распространения персональных данных в общедоступных источниках.

Форма и порядок осуществления регистрации и учета законодателем не определены. Организация может соблюдать это требование, например, посредством ведения журнала в электронной или бумажной форме.

## 9. Как государство контролирует исполнение законодательства о защите персональных данных?

Несмотря на то, что требования в части сбора, обработки и защиты персональных данных были введены в Казахстане в 2013 году с принятием Закона о персональных данных, государственный орган, уполномоченный осуществлять контроль за соблюдением законодательства в соответствующей части (Министерство цифрового развития, инноваций и аэрокосмической промышленности Казахстана), и его компетенция были определены законодателем только в 2020 году. К компетенции уполномоченного органа, помимо прочего, относятся следующие функции:

- рассмотрение обращений субъектов и их законных представителей по вопросам проверки соответствия содержания персональных данных и способов их обработки целям их обработки;
- принятие мер по привлечению лиц, допустивших нарушения законодательства Казахстана о персональных данных и их защите, к ответственности;
- право требовать от собственника, оператора и третьих лиц уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных.

Общий надзор за соблюдением законности в сфере защиты персональных данных осуществляют органы прокуратуры. В целях защиты своих прав и привлечения виновных лиц к ответственности субъектам необходимо обращаться в

вышеуказанные органы, которые при подтверждении нарушений будут применять к виновным лицам меры ответственности.

Следует иметь в виду, что в рамках установленного законодательством Казахстана механизма по выявлению и пресечению нарушений в сфере защиты персональных данных негативные последствия для оператора могут возникнуть только в результате конфликта между оператором и субъектом относительно собранных и обрабатываемых персональных данных и последующего обращения субъекта в уполномоченные органы за защитой своих прав. Плановые проверки организаций на предмет соблюдения требований по защите персональных данных законодательством не предусмотрены.

## 10. Какая ответственность установлена за нарушение законодательства о защите персональных данных?

За несоблюдение мер по защите персональных данных, а также за их незаконные сбор и обработку законодательство Казахстана предусматривает административную ответственность в виде штрафа, размер которого зависит от категории правонарушителя и квалифицирующих признаков и варьируется от 10 до 1 000 месячных расчетных показателей (на момент подготовки настоящего материала размер МРП составляет 3 063 тенге).

В отношении длящихся нарушений, не устраненных на момент выявления, уполномоченными органами может быть издано предписание об их устранении. Если такое предписание не будет выполнено правонарушителем, он может быть привлечен к административной ответственности уже за невыполнение предписаний уполномоченного органа в виде штрафа в размере от 5 до 500 МРП и потенциального приостановления действия разрешения на определенный вид деятельности либо приостановления деятельности правонарушителя (отдельных видов его деятельности).

В том случае, если несоблюдение мер по защите персональных данных повлекло причинение существенного ущерба, виновные (только физические) лица могут быть привлечены к уголовной ответственности в виде штрафа (в размере до 3 000 МРП), привлечения к исправительным работам (в том же денежном размере), привлечения к общественным работам (на срок до 600 часов), ограничения свободы (на срок до 2 лет) или лишения свободы (на тот же срок) с потенциальным лишением права занимать определенные должности либо заниматься определенной деятельностью.

Кроме того, субъект (его законный представитель) вправе взыскать с правонарушителя причиненные нарушением убытки, в том числе моральный ущерб, в судебном порядке.

• • •