ТИПИЧНЫЕ НАРУШЕНИЯ ЗАКОНОДАТЕЛЬСТВА О ПЕРСОНАЛЬНЫХ ДАННЫХ

ДИСКО В.И.,
заместитель начальника управления контроля и аудита Национального центра защиты персональных данных Республики Беларусь

Обязательные меры по обеспечению защиты персональных данных, предусмотренные п. 3 ст. 17 Закона Республики Беларусь от 7 мая 2021 г. №99-З «О защите персональных данных» (далее – Закон), составляют «сердцевину» мероприятий, принимаемых оператором для обработки персональных данных в соответствии с требованиями Закона.

Закон не раскрывает, каким образом должны быть реализованы обязательные меры по обеспечению защиты персональных данных, равно как и не определяет недопустимые способы их принятия. Указанное позволяет оператору самостоятельно определять способы и возможные варианты реализации таких мер с учетом специфики его деятельности, количества бизнес-процессов, масштабов обработок персональных данных и т.д.

В целях оказания операторам помощи по реализации указанных мер Национальным центром защиты персональных данных (далее – НЦЗПД) подготовлено множество рекомендаций и разъяснений о применении законодательства о персональных данных, проведен ряд обучающих мероприятий (семинаров, вебинаров и др.).

Вместе с тем, как показывает анализ проводимой НЦЗПД контрольной деятельности, на практике операторы продолжают допускать нарушения при реализации обязательных мер по обеспечению защиты персональных данных. Многие из таких нарушений носят типичный характер, поскольку выявляются у операторов (уполномоченных лиц) вне зависимости от масштабов обработки персональных данных, сфер их деятельности, а также имеющихся ресурсов.

В соответствии с положениями Указа Президента Республики Беларусь от 28 октября 2021 г. №422 «О мерах по совершенствованию защиты персональных данных» НЦЗПД при осуществлении контроля в обязательном порядке делает вывод о достаточности принятых мер для защиты персональных данных и их соответствии требованиям законодательства о персональных данных. При этом нередко в актах, оформляемых по итогам проведенных проверок, указывается, что принятые оператором меры по обеспечению защиты персональных данных являются недостаточными для защиты персональных данных по причине формального подхода к их реализации.

В ходе проверок НЦЗПД осуществляется оценка соответствия законодательству о персональных данных не только локальных правовых актов и иных документов оператора, но также значительное внимание уделяется фактическому положению дел по обеспечению защиты (например, путем бесед с работниками оператора, анализом информационных ресурсов (систем)). К сожалению, обобщение результатов контрольной деятельности свидетельствует иногда о значительном разрыве между положениями локальных правовых актов оператора и фактическим положением дел в отношении обработки персональных данных.

Закон устанавливает ряд мер, обязательных для всех операторов (уполномоченных ими лиц). Согласно п. 3 ст. 17 Закона такими мерами являются:

1) назначение оператором (уполномоченным лицом), являющимся государственным органом, юридическим лицом Республики Беларусь, иной организацией, структурного подразделения или лица, ответственного за осуществление внутреннего контроля за обработкой персональных данных (далее – внутренний контроль).

Ненадлежащая реализация данной меры является причиной отсутствия (неэффективной реализации) оператором обязательных мер по обеспечению защиты персональных данных, а также иных мер, подлежащих принятию в соответствии с законодательством о персональных данных (например, подготовка форм согласий, внесение сведений в реестр операторов и т.п.).

По этой причине важно, чтобы такое лицо (структурное подразделение) имело достаточные ресурсы (организационные, временные и т.п.) для эффективного исполнения своих функций, а также обладало независимостью для беспрепятственного установления нарушений при осуществлении внутреннего контроля.

Если в первое время после принятия Закона НЦЗПД выявлялись нарушения при реализации этой меры, связанные в основном с отсутствием такого лица (структурного подразделения), то сейчас такое лицо (структурное подразделение) большинством операторов назначено. При анализе вариантов назначения лица (структурного подразделения) НЦЗПД зачастую указывает на неэффективную форму ее реализации:

● назначение лица (структурного подразделения), осуществляющего на постоянной основе обработку персональных данных значительного количества субъектов персональных данных. Такое назначение может приводить к конфликту интересов (совпадение в одном лице контролера и контролируемого), т.е. ситуации, при которой основные должностные обязанности лица (например, руководителя кадровой службы либо работника службы безопасности оператора) помешают эффективному осуществлению деятельности по внутреннему контролю, которая отходит на второй план. Наличие конфликта интересов должно оцениваться в каждом случае индивидуально, исходя из численности работников организации и наличия иных работников, способных эффективно выполнять соответствующие обязанности (например, в микроорганизациях (до 15 человек) иных вариантов, кроме возложения обязанностей на руководителя, не имеется);

● формальное возложение обязанностей по осуществлению внутреннего контроля на одного из работников, который не имеет объективной возможности выполнять соответствующие функции (например, с учетом уже имеющихся должностных обязанностей) либо знания законодательства о персональных данных (что, как правило, предполагает наличие юридического образования) и практики его применения. Такими работниками могут быть: в первом случае единственный юрисконсульт в крупной организации, который осуществляет масштабную обработку персональных данных, а во втором случае – главный бухгалтер в небольшой организации;

● назначение лица, а не структурного подразделения при осуществлении оператором масштабной обработки персональных данных (значительное количество клиентов или работников, большой перечень обрабатываемых персональных данных) либо обработки персональных данных при реализации сложных бизнес-процессов (например, привлечение множества уполномоченных лиц из различных юрисдикций, деятельность которых необходимо контролировать);

● отсутствие прямого подчинения лица (подразделения) руководителю (у крупных операторов – заместителю руководителя). В отдельных организациях такое лицо может входить в состав отдела, который является одним из структурных подразделений управления, подчиняющегося заместителю руководителя оператора. Необходимость согласования принимаемых решений с «вертикалью» руководителей свидетельствует об отсутствии независимости такого лица, поскольку каждый руководитель может заблокировать принятие необходимых мер по причине конфликта интересов (нередко принимаемые меры по обеспечению защиты персональных данных влекут необходимость пересмотра бизнес-процессов, трату ресурсов, дополнительные обязанности (ограничения) для работников).

Следствием таких неэффективных вариантов назначения во всех случаях являлось то, что лицо (структурное подразделение) было не в состоянии обеспечить реализацию иных требований Закона (например, подготовку требуемых локальных правовых актов, контроль за обработкой персональных данных уполномоченными лицами, рассмотрение заявлений субъектов персональных данных и т.п.).

Кроме того, при оценке рассматриваемой обязательной меры по обеспечению защиты персональных данных иногда выявляются случаи фактического непроведения внутреннего контроля, что подтверждается отсутствием документов о его проведении (порядка проведения, докладных записок, отчетов по итогам проведения) и пояснениями как ответственного за осуществление внутреннего контроля, так и иных работников (например, работники не могут указать примерный период проведения контроля, объекты контроля, а также его основные итоги, в т.ч. выявленные в их деятельности недостатки).

При этом принятие локального правового акта, определяющего порядок и план проведения внутреннего контроля, должно иметь своей целью не столько выявление нарушений, сколько их предупреждение. Иными словами, работники оператора, зная порядок проведения внутреннего контроля, его период, объекты, подлежащие контролю, могут провести анализ своей деятельности и исключить нарушения до их выявления соответствующим лицом (структурным подразделением);

2) издание оператором (уполномоченным лицом), являющимся юридическим лицом Республики Беларусь, иной организацией, индивидуальным предпринимателем, документов, определяющих политику оператора (уполномоченного лица) в отношении обработки персональных данных.

Указанная мера направлена на реализацию положений п. 6 ст. 4 Закона о прозрачном характере обработки персональных данных и призвана дать субъекту персональных данных понимание порядка и пределов обработки его персональных данных оператором. В свою очередь, издание отдельными операторами документов, определяющих его политику в отношении обработки персональных данных (далее, если не указано иное, – политика), которые не позволяют достичь указанной цели, свидетельствуют о формальном исполнении требований Закона.

Типичными нарушениями при реализации указанной меры являются:

● отсутствие соотношения в политике целей обработки, категорий субъектов персональных данных, чьи данные подвергаются обработке, перечня обрабатываемых персональных данных (в частности, цели обработки, категории субъектов персональных данных, перечень обрабатываемых сведений, правовые основания изложены в различных пунктах документа). Такое положение дел возлагает на субъекта персональных данных бремя самостоятельного соотношения целей обработки с правовым основанием и перечнем обрабатываемых персональных данных и в целом лишает понимания, как его персональные данные обрабатываются в конкретной ситуации;

● отсутствие указания в политике на все бизнес-процессы, в ходе которых осуществляется обработка персональных данных (например, отсутствие политики по обработке персональных данных в трудовых отношениях либо при осуществлении видеонаблюдения и т.п.);

● принятие одного документа, определяющего политику оператора в отношении обработки персональных данных, в случае масштабной обработки персональных данных либо изложение его сложным юридическим или техническим языком, исключающим понимание его субъектами персональных данных, чьи данные обрабатываются в соответствии с этой политикой (например, одним из операторов подготовлена политика на 55 страниц в отношении 51 бизнес-процесса одновременно как работников, так и клиентов). Такой документ, как правило, сложен для восприятия, что фактически нивелирует эффект от его принятия и нарушает требования о прозрачном характере обработки персональных данных (п. 6 ст. 4 Закона).

К числу типичных недостатков при издании политики следует также отнести:

● отсутствие информации о правовых основаниях обработки персональных данных (зачастую оператор указывает только на возможность обработки на основании согласия), сроках обработки, об уполномоченных лицах, трансграничной передаче персональных данных, правах субъектов персональных данных и механизме их реализации и иной информации, необходимой для обеспечения прозрачности процесса обработки персональных данных;

● указание слишком общих либо неконкретных целей обработки (обеспечение соблюдения законодательства, осуществление своей деятельности в соответствии с уставом) и неконкретных сроков («согласие действует до момента отзыва этого согласия либо до момента, установленного законодательством»);

● неуказание механизма реализации прав субъектов персональных данных, в т.ч. неуказание лица (структурного подразделения), ответственного за осуществление внутреннего контроля;

● возложение на субъектов персональных данных обязанностей, не предусмотренных Законом (досудебный порядок разрешения споров);

● излишнее дублирование положений Закона (например, ст. 6), приведение положений, изложенных с учетом подходов российского или европейского законодательства (например, обработка персональных данных на основании легитимного интереса), использование «типовых» политик;

● несоответствие положений политики бизнес-процессам оператора;

● несогласованность положений политики и прямое противоречие их друг другу;

● опубликование на разных страницах интернет-сайта разных версий политик (например, выявлен случай, когда на сайте оператора было размещено три разных версии политики).

В целом надлежащая реализация данной меры является отражением проводимой оператором работы по систематизации обработок персональных данных (ведение реестра обработок) и позволяет

провести ревизию бизнес-процессов, исключив возможные нарушения (обработку персональных данных без наличия правовых оснований, избыточную обработку и т.п.);

3) ознакомление работников оператора (уполномоченного лица) и иных лиц, непосредственно осуществляющих обработку персональных данных, с положениями законодательства о персональных данных, в т.ч. с требованиями по защите персональных данных, документами, определяющими политику оператора (уполномоченного лица) в отношении обработки персональных данных, а также обучение указанных работников и иных лиц в порядке, установленном законодательством.

Нередко действия работников оператора (уполномоченного лица) являются поводом для направления субъектами персональных данных жалоб в НЦЗПД. При этом в ряде случаев несоответствие таких действий требованиям законодательства о персональных данных не является очевидным для работника. Так, иногда работник не знает (но должен знать), что нарушает требования Закона. В связи с этим надлежащая реализация этой обязательной меры представляет для оператора особую важность, поскольку минимизирует его риски по нарушению Закона из-за «человеческого» фактора.

Типичными нарушениями при реализации указанной меры являются:

● нереализация рассматриваемой меры либо ознакомление с информацией лишь отдельных работников, которые обрабатывают персональные данные (например, только кадровой службы);

● ознакомление с неполным объемом требуемой информации (например, ознакомление только с положениями законодательства о персональных данных без изучения документов, определяющих политику оператора в отношении обработки персональных данных);

● формальный подход к реализации указанной меры (неэффективный способ ознакомления – размещение на информационных стендах организации либо рассылка посредством корпоративной почты с указанием на необходимость его самостоятельного изучения) без реального обучения с контролем знаний (в форме опроса, тестирования и других формах контроля знаний);

● ознакомление и обучение носит чрезмерно общий характер без учета трудовой функции работника. Примером такой ситуации может быть контроль знаний в форме теста, состоящего из 10 вопросов, посвященных истории принятия Закона, обязательным мерам по обеспечению защиты персональных данных для работника, который получает согласия субъектов персональных данных на обработку их персональных данных. При этом вопросы, связанные с порядком получения (отзыва) согласия, а также с иной информацией, предоставляемой в соответствии со ст. 5 Закона, отсутствуют.

Как формальный подход к реализации данной меры рассматривается случай, когда, несмотря на представленные документы о ее реализации (например, лист ознакомления с подписями работников и протокол сдачи теста), работники не владеют базовыми положениями законодательства о персональных данных либо вовсе прямо указывают на то, что ознакомление и обучение фактически не проводилось;

4) установление порядка доступа к персональным данным, в т.ч. обрабатываемым в информационном ресурсе (системе).

Типичными нарушениями при реализации указанной меры являются:

● отсутствие порядка доступа к персональным данным;

● определение порядка доступа лишь применительно к информационным ресурсам (системам) (в частности, порядок доступа в отношении обработки персональных данных на бумажных носителях отсутствует);

● установление перечня лиц (должностей, структурных подразделений), осуществляющих обработку персональных данных, без указания бизнес-процессов, при реализации которых такой доступ необходим;

● несоответствие установленного порядка реальному положению дел по разграничению прав доступа к персональным данным, обрабатываемым в информационном ресурсе (системе);

5) осуществление технической и криптографической защиты персональных данных в порядке, установленном Оперативно-аналитическим центром при Президенте Республики Беларусь, в соответствии с классификацией информационных ресурсов (систем), содержащих персональные данные.

Нарушением при реализации указанной меры является неосуществление технической и криптографической защиты персональных данных в порядке, установленном Положением о порядке аттестации систем защиты информации информационных систем, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, утвержденным приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 20 февраля 2020 г. №66.

В целом надлежащая реализация обязательных мер по обеспечению защиты персональных данных имеет важное практическое значение, поскольку рассматривается как сформированный оператором фундамент по исполнению требований законодательства о персональных данных, снижает риски привлечения к ответственности (что с учетом назревшей необходимости ее усиления в ближайшие несколько лет повышает актуальность), финансовых и имиджевых потерь.

V.I.DISKO

Typical law violations on Personal Data