

Чек-лист по оценке привлекаемых уполномоченных лиц

1. Согласно абзацу четвертому пункта 1 статьи 16 Закона Республики Беларусь от 7 мая 2021 г. № 99-З "О защите персональных данных" (далее – Закон) оператор обязан обеспечивать защиту персональных данных в процессе их обработки.

Пунктом 1 статьи 17 Закона эта обязанность конкретизирована в виде необходимости принятия им правовых, организационных и технических мер по обеспечению защиты персональных данных от несанкционированного или случайного доступа к ним, изменения, блокирования, копирования, распространения, предоставления, удаления персональных данных, а также от иных неправомерных действий в отношении персональных данных.

В случае поручения обработки персональных данных уполномоченному лицу ответственность перед субъектом персональных данных за действия указанного лица несет оператор. Уполномоченное лицо несет ответственность перед оператором (пункт 3 статьи 7 Закона).

Таким образом, оператор обязан привлекать к обработке персональных данных только тех уполномоченных лиц, которые во исполнение положений статьи 17 Закона принимают правовые, организационные и технические меры по обеспечению защиты персональных данных. Привлечение оператором уполномоченных лиц, которые не реализуют указанные меры вовсе, либо неосуществление оценки их реализации уполномоченными лицами (даже, если они закреплены в договоре) не согласуются с требованиями Закона, поскольку не позволяют операторам эффективно выполнять свою обязанность по обеспечению защиты персональных данных.

2. Выбор "подрядчика", привлекаемого для бизнес-процессов, в ходе которых ему будет поручена обработка персональных данных, должен осуществляться как с учетом принимаемых им мер по обеспечению защиты персональных данных, так и возможности эффективного выполнения оператором своих обязанностей, предусмотренных пунктом 1 статьи 16 Закона (например, по удалению данных, рассмотрению заявлений субъектов персональных данных, уведомлению о нарушении систем защиты персональных данных и т.п.).

Оператору следует принимать разумные усилия по изучению указанных вопросов. Это может быть сделано, например, путем анализа интернет-сайта уполномоченного лица (в ходе которого изучаются документы, определяющие его политику в отношении обработки персональных данных), коммуникации с лицом, ответственным за осуществление внутреннего контроля, направления чек-листа с предложением дать ответы (предоставить документы) по вопросу реализации мер в соответствии со статьей 17 Закона (см. приложение).

На практике операторами зачастую запрашиваются конкретные документы, подтверждающие реализацию уполномоченными лицами мер по обеспечению защиты персональных данных (например, порядок доступа к персональным данным, результаты обучения работников уполномоченного лица, подтверждение осуществления внутреннего контроля), что воспринимается уполномоченными лицами как вмешательство в свои внутренние процессы и в отдельных случаях препятствует заключению договора, предусмотренного статьей 7 Закона.

В этой связи не противоречит законодательству о персональных данных подход по изучению реализации этих мер как путем запроса конкретных документов (выписок из них), так и путем получения сведений об их реализации (без предоставления копий документов).

Отдельные уполномоченные лица "уклоняются" от предоставления информации о реализации мер по обеспечению защиты персональных данных, привлекаемых субуполномоченных лицах, осуществлении трансграничной передачи персональных данных, ссылаясь на конфиденциальность этих сведений. Однако эти сведения необходимо предоставлять оператору в целях эффективного выполнения им предусмотренных статьей 16 Закона обязанностей.

3. Важно отметить, что Закон не исключает возможности привлечения уполномоченного лица, которое не реализует (ненадлежаще реализует) отдельные из обязательных мер по обеспечению защиты персональных данных.

С учетом риск-ориентированного подхода, следующего из пункта 2 статьи 17 Закона, возможность поручения обработки персональных данных уполномоченному лицу оценивается оператором в каждом конкретном случае индивидуально с учетом реализованных им мер, характера поручаемой обработки персональных данных и иных складывающихся у него обстоятельств, связанных с такой обработкой.

При этом она может не ограничиваться изучением исключительно обязательных мер, предусмотренных пунктом 3 статьи 17 Закона.

Так, например, осуществление технической поддержки приложения, посредством которого собираются специальные персональные данные (сведения о состоянии здоровья), дополнительно требует от оператора изучения вопросов принятия уполномоченным лицом комплекса мер, направленных на предупреждение рисков, которые могут возникнуть при обработке таких персональных данных для прав и свобод субъектов персональных данных (пункт 3 статьи 8 Закона), а также назначения лица (структурного подразделения), ответственного за обеспечение защиты информации.

Соответственно, исходя из складывающегося на практике многообразия отношений (обстоятельств), исчерпывающий перечень мер (документов), подлежащих изучению оператором при привлечении уполномоченных лиц, установить законодательно не представляется возможным.

4. Учитывая, что отношения по поручению обработки персональных данных могут носить длительный характер, оператору следует в течение срока действия договора осуществлять контроль за реализацией уполномоченными лицами мер по обеспечению защиты персональных данных, в том числе обязательных, предусмотренных пунктом 3 статьи 17 Закона.

Кроме того, оператору оправданно убеждаться в своей возможности эффективного исполнения иных обязанностей, предусмотренных пунктом 1 статьи 16 Закона (например, осуществлять контроль за прекращением обработки персональных данных (посредством личного кабинета на сайте уполномоченного лица либо получением информации о таком прекращении) при отсутствии оснований для обработки персональных данных).

Порядок (формы, периодичность и т.п.) такого контроля могут быть закреплены в поручении (договоре, соглашении) на обработку персональных данных.

В свою очередь, если бизнес-процесс для уполномоченного лица является типовым, то документы, подтверждающие реализацию мер, могут быть опубликованы на его интернет-сайте либо быть доступны для скачивания в личном кабинете.

В случае прекращения договорных отношений оператор должен иметь возможность подтвердить, что уполномоченное лицо прекратило порученную ему обработку персональных данных. Такое прекращение может быть оформлено соответствующим актом или отчетом.

5. Представленный чек-лист позволит оператору очертить круг вопросов, которые могут быть изучены им при привлечении уполномоченных лиц, а также их важности для эффективного выполнения обязанности по обеспечению защиты персональных данных. Изучаемые меры, как и предлагаемая базовая методика их оценки (прилагается), являются ориентиром для оператора и могут быть адаптированы с учетом своей деятельности (в рамках "риск-ориентированного подхода").