

Почему важно?

Проект представляет собой первое комплексное правовое регулирование в сфере персональных данных и вводит новые категории в белорусское законодательство.

В Беларуси и в настоящее время есть достаточно норм в части режима персональных данных, однако действующее регулирование можно назвать «спящим»: при отсутствии прямой ответственности на практике многие организации не выполняют его требования без критических для себя последствий. После принятия Проекта компаниям придется значительно пересмотреть свои бизнес-процессы во избежание санкций со стороны государства и взыскания убытков со стороны физических лиц.

Что общего с ЕС и РФ?

При разработке учтен подход Общего регламента по защите данных ЕС (GDPR), хотя имеются и значимые отличия. В частности, нет такого четкого деления на «контролеров» (data controller) и «процессоров» (data processor) с аналогичным распределением ответственности перед субъектом данных.

В целом разработка Проекта отвечает общему подходу в регулировании защиты информации в Российской Федерации, где действует Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации», в развитие которого принят специальный Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных». В то же время в Беларуси пока нет специальных положений касательно персональных данных работников, закрепленных, к примеру, в Трудовом кодексе Российской Федерации. Главным отличием Проекта по существу является отсутствие требования о локализации серверов.

Справочно.

GDPR (General Data Protection Regulation) — Общий регламент по защите данных (Регламент ЕС 2016/679 от 27 апреля 2016 г.), вступивший в силу с 25 мая 2018 г.

А кто в главных ролях?

Главными действующими субъектами являются оператор и субъект персональных данных. В качестве оператора выступают лица, осуществляющие операции с персональными данными, а в качестве субъектов — лица, в отношении которых осуществляются такие операции. На наш взгляд, для внесения определенности можно уточнить, будет ли Проект распространять свое действие на иностранных физических лиц, находящихся на территории Республики Беларусь, или на иностранных лиц, осуществляющих операции с персональными данными граждан Республики Беларусь. Кроме этого, оператор может поручать действия с персональными данными другому лицу на основании договора либо решения государственного органа. Такой «субподрядчик» несет ответственность перед оператором, но не перед субъектом персональных данных напрямую.

Справочно.

В Проекте оператор определен как государственный орган, физическое лицо, индивидуальный предприниматель, юридическое лицо Республики Беларусь, осуществляющие сбор, обработку, распространение, предоставление персональных данных.

Для чего особый правовой режим?

Проект определяет категорию «специальных персональных данных» и особый правовой режим для их защиты. Так, операции со специальными персональными данными по общему правилу не допускаются, за исключением прямо закрепленных в Законе случаев (например, для исполнения судебного постановления или если сам субъект сделал данные общедоступными). Биометрические и генетические персональные данные выделяются как подкатегории специальных, хотя самостоятельно не используются в Проекте.

В качестве возможных операций с персональными данными в Проекте перечисляются «обработка», «сбор», «распространение» и «предоставление» как равнозначные, что не вполне согласуется с международными подходами и усложняет их использование на практике. При этом из конструкции норм Проекта не вытекает, с чем связано такое обособление обработки (как общей категории) от иных специальных действий с персональными данными.

Где хранить персональные данные?

Одним из преимуществ Проекта является отсутствие требования о локализации хранения персональных данных в базах данных, находящихся на территории Республики Беларусь. Такой подход позволяет иностранным операторам производить действия с персональными данными на серверах, расположенных за пределами страны (облачные ресурсы), а белорусским операторам — осуществлять трансграничную передачу персональных данных при условии обеспечения в другом государстве надлежащего уровня их защиты, кроме специально определенных случаев (например, в случае заключения договора с субъектом персональных данных).

Так, согласно ч. 5 ст. 18 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» при сборе персональных данных, в том числе посредством сети Интернет, оператор обязан обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан с использованием баз данных, находящихся на территории Российской Федерации. На основании данной нормы в России был заблокирован доступ к LinkedIn.

Перечень стран с надлежащим уровнем защиты определит уполномоченный орган по защите прав субъектов персональных данных.

Наказывать будут рублем?

Операторы обязаны назначить ответственное лицо по защите персональных данных, которое будет отвечать за организацию операций с персональными данными. В случае, если защита персональных данных нарушена, оператор обязан не позднее 3 дней после обнаружения утечки сообщить об этом уполномоченному органу, за исключением случая незначительной утечки.

На данный момент размер административных штрафов не определен. Проект также предусматривает, что нарушитель будет возмещать моральный вред наряду с имущественным вредом и понесенными убытками.

Кто уполномоченный орган?

Проект предоставляет полномочия Президенту по определению уполномоченного органа и утверждению положения о таком органе.

Внесение на рассмотрение положения об уполномоченном органе поручено осуществить Совету Министров Республики Беларусь после официального опубликования Проекта.

Проект не вносит ясности относительно предполагаемого места уполномоченного органа в системе госорганов. При этом надзор за исполнением законодательства о персональных данных возлагается на Генеральную прокуратуру.

Как будут просить согласие?

Проект решает вопрос с формой получения согласия: она может быть письменной, в виде электронного документа и в иной электронной форме. Если второй вариант требует наличия электронной цифровой подписи, то последний вариант более практичен и, главное, должен позволять установить факт получения согласия.

Примеры получения согласия в электронной форме:

- указание субъектом персональных данных определенной информации (кода) после получения СМС-сообщения или сообщения на адрес электронной почты;
- простановка субъектом персональных данных галочки или иной отметки на интернет-ресурсе (чек-бокс).

Субъекту предоставляется право отозвать свое согласие на обработку данных в той форме, в которой оно было дано.

Какой порядок действует сейчас?

На данный момент регулирование персональных данных содержится:

— в Законе Республики Беларусь от 10.11.2008 № 455-З «Об информации, информатизации и защите информации» (далее — [Закон об информации](#)⁹);

— в Законе Республики Беларусь от 21.07.2008 № 418-З «О регистре населения» (далее — [Закон о регистре](#)⁹).

Значение [Закона о регистре](#)⁹ в сфере персональных данных, кроме регулирования в рамках специфики его назначения, состоит в закреплении перечня основных и дополнительных персональных данных и, по сути, этим ограничивается.

[Закон об информации](#)⁹ содержит общие положения в отношении регулирования защиты персональных данных. Развитие его положений осуществляется Оперативно-аналитическим центром при Президенте Республики Беларусь (ОАЦ) путем издания приказов. В частности, приказ ОАЦ от 30.08.2013 № 62 устанавливает требования к проектированию, созданию и эксплуатации информационных систем, предназначенных для обработки персональных данных.

Общий подход закреплён в [ст. 29 Закона об информации](#)⁹, которая предусматривает правовые, организационные и технические меры защиты в отношении персональных данных с момента, когда они были предоставлены физическим лицом. Персональные данные относятся к информации, распространение или предоставление которой ограничено (информации ограниченного распространения), согласно абз. 2 ч. 1 [ст. 17 Закона об информации](#)⁹ и, соответственно, подпадают под требования к работе с такой информацией.

Меры защиты информации

