О подходах по минимизации выполнения требований закона «О персональных данных»

Валерий Омаров
К.т.н.,
руководитель группы анализа и защиты информации СОАО «ВСК»

Введение

Защита персональных данных в связи с требованиями федерального закона №152-ФЗ «О персональных данных» (далее - закон) в последнее время занимает умы не только специалистов IT-подразделений, но и всех граждан, чьи персональные данные закон охраняет.

С одной стороны, с принятием закона, значительно вырос рынок услуг по обеспечению информационной безопасности, технических и программных средств защиты. С другой стороны, для операторов персональных данных наступили тяжелые времена. И чем более не проработаны вопросы защиты персональных данных в законе и подзаконных актах, тем сложнее их защитить.

Поэтому актуальной проблемой остается вопрос минимизации затрат по защите персональных данных в соответствии с требованиями закона «О персональных данных».

В статье рассматриваются подходы для оптимизации мер, применяемых для защиты персональных данных, не требующих внедрения сертифицированных технических и программных средств - обезличивание и отнесения персональных данных к общедоступным.

Конфиденциальность персональных данных

В ст. 3 п.10 Федерального закона «О персональных данных» №152-ФЗ дано определение конфиденциальности персональных данных - обязательное соблюдение оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания. В данном определении конфиденциальность персональных данных рассматривается в широком смысле: указан явный запрет на передачу персональных данных третьим лицам без согласия её обладателя и указана необходимость предотвращения утечки (разглашения) какой-либо информации о субъекте. Оператор должен на 100% обеспечить не распространение персональных данных.

В ст.7. закона раскрывается, когда не требуется обеспечение конфиденциальности персональных данных:

1) в случае обезличивания персональных данных;

2) в отношении общедоступных персональных данных.

Обезличивание

Обезличивание персональных данных - действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных. Например, по номеру телефона страхователя и данных об его автомобиле невозможно определить субъекта персональных данных.

Обезличенные персональные данные относятся к 4-й категории персональных данных, конфиденциальность для которых обеспечивать не нужно. Требований к «правильному» обезличиванию не существует и способы (алгоритмы) обезличивания персональных данных оператор, осуществляющий обработку персональных данных, определяет самостоятельно.

Обезличивание возможно несколькими способами:

- использование системы «диспергированных идентификационных данных», когда часть ключевых идентификационных данных вручается их владельцам [3];
- сокращение перечня обрабатываемых сведений, (например, передача списков «обзвона» страхователей только с номерами телефонов и данных об объекте страхования);
- использование алгоритмов обезличивания, например, k-анонимность, предложенные Латаньей Суинни [5];
- замена части сведений идентификаторами, например, кодами болезней;
- дискретизация - замена численных значений диапазоном (например, стаж вождения до 1 года);
- обобщение - понижение точности некоторых сведений;
- шифрование персональных данных;
- алгоритмы перемешивания данных и др.

Трудности. Процесс обезличивания сложен и зависит от бизнес-процессов. Изменение бизнес-процессов может привести к пересмотру способа обезличивания. И самое главное, что делать, если процедура обезличивания не пройдет одобрения у регулятора?

Положительные моменты. Упрощение самих бизнес-процессов за счет экономии перечня обрабатываемых данных. Понижение класса информационной системы персональных данных (далее – ИСПДн). Значительная экономия финансовых средств.

В любом случае способы обезличивания надо использовать, и применительно к отраслям деятельности по возможности провести стандартизацию для решения проблем с регуляторами.

Например, рассмотрим бизнес-процесс пролонгации договоров страхования транспортных средств (звонок клиенту - напоминание о пролонгации). Определим перечень персональных данных для осуществления пролонгации: номер телефона, марка автомобиля, дата окончания полиса. Для выполнения такого бизнес-процесса достаточно иметь информационную систему персональных данных класса К4.

В этом случае:

- при обработке персональных данных как в автоматизированном, так и неавтоматизированном режимах не требуется использовать технические средства защиты;
- не требуется выполнять весь комплекс организационно-методических мероприятий по защите персональных данных. Достаточно провести классификацию ИСПДн путем рассмотрения ИСПДн на внутриведомственной комиссии с изданием Акта о классификации ИСПДн.
- на жалобы об утечках информации (для нашего примера – ряд звонков страхователю от работников других страховых компаний о пролонгации договора страхования автомобиля) мы можем обоснованно ответить, что данные являются обезличенными и могут свободно находиться на любых сайтах, а для аргументации приложить Акт о классификации своей ИСПДн.

Данный подход (обезличивание) позволяет сегментировать информационную систему таким образом, чтобы минимизировать защиту информационной системы компании.

При обезличивании необходимо придерживаться ряда принципов:

1. если некоторый атрибут (например, номер телефона) входит в некую справочно - информационную систему, которая содержит такие персональные данные как фамилию, имя, адрес проживания и иные персональные данные, и не относится к общедоступным источникам персональных данных, то этот атрибут считаем обезличенным;
2. комбинация таких обезличенных атрибутов как СНИЛС, ИНН, номер паспорта и др. не приводят к деобезличиванию; также как и добавление их к другим обезличенным персональным данным;
3. в связи с отсутствием допустимых значений вероятностей определения субъекта по комбинации персональных данных опираемся на правила обезличенных совокупностей. Например, правило №1 - совокупность персональных данных: фамилия, имя, отчество, год рождения – обезличенные данные;
4. меньшая совокупность обезличенной совокупности также обезличена и др.

Используя данный подход можно легко минимизировать защиту информационной системы.

Выводы:

1.В связи с отсутствием требований к «правильному» обезличиванию оператор, осуществляющий обработку персональных данных, может определять их самостоятельно.

2.Для обезличивания годятся любые методы и способы явно не запрещенные законодательно.

3.Необходимо постоянно пересматривать состав персональных данных и методы их защиты с целью оптимизации требований по защите персональных данных.

Общедоступные персональные данные

Общедоступные персональные данные - персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

Общедоступные персональные данные относятся к 4-й категории персональных данных, конфиденциальность для которых обеспечивать не требуется.

При обработке общедоступных персональных данных обязанность доказывания того, что обрабатываемые персональные данные являются общедоступными, возлагается на оператора. Из этого следует, что для обработки общедоступных данных требуется доказательство, что они являются общедоступными или требуется получить согласие субъекта. Закон (п.4 ст.9) предусматривает обработку персональных данных только с согласия в письменной форме субъекта персональных данных. Причем письменное согласие субъекта персональных данных на обработку своих персональных данных должно включать в себя:

1) фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

2) наименование (фамилию, имя, отчество) и адрес оператора, получающего согласие субъекта персональных данных;

3) цель обработки персональных данных;

4) перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

5) перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;

6) срок, в течение которого действует согласие, а также порядок его отзыва;

7) собственноручную подпись субъекта персональных данных.

Рассмотрим в качестве примера соглашение о конфиденциальности, заключаемое с субъектом:

«*Я (ФИО полностью), паспорт (иной документ, удостоверяющий личность) серия___№____, выдан (кем и когда), проживающий по*

адресу_____, дата рождения (число/месяц/год), контактный телефон_____ настоящим подтверждаю свое согласие на обработку Страховщиком и партнерами Страховщика моих персональных данных в целях заключения и реализации Договора страхования, а также в целях соблюдения требований действующего законодательства.

Для целей настоящего Договора страхования мои персональные данные включают в себя: фамилию, имя, отчество, дату рождения, адрес проживания, контактный телефон, паспортные данные, сведения о состоянии здоровья, заболеваниях и об обращениях в медицинские учреждения.

Страховщик вправе осуществлять все необходимые действия с моими персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, передачу партнерам (медицинским и иным учреждениям, с которыми у Страховщика имеются договорные отношения об оказании медицинской и иной помощи), получение данных обо мне от партнеров Страховщика, обезличивание, блокирование, уничтожение, внесение в информационную систему, обработку с использованием средств автоматизации или без использования таких средств. Страховщик может осуществлять обработку моих персональных данных в течение действия Договора страхования и в течение 5 (пяти) лет после его прекращения.

Я понимаю и согласен с тем, что при передаче моих персональных данных Страховщику, работники медицинских и иных учреждений освобождаются от обязательств конфиденциальности перед Страховщиком. При этом передача моих персональных данных иным лицам или их разглашение может осуществляться только с моего письменного согласия.

Я вправе отозвать свое согласие на обработку персональных данных посредством соответствующего письменного заявления, которое должно быть направлено Страхователю заказным письмом с уведомлением о вручении либо передано под расписку представителю Страхователя. В случае получения от Страхователя такого письменного заявления, Страховщик расторгает Договор страхования в отношении данного Застрахованного с дальнейшим прекращением медицинского обслуживания. Данное согласие передано мной в момент подписания Договора страхования».

При заключении вышеприведенного соглашения требуется выполнять все меры по соблюдению конфиденциальности персональных данных.

Но если добавить фразу: «*все передаваемые мною персональные данные в рамках Договора согласен считать общедоступными персональными данными»,* то в этом случае конфиденциальность персональных данных обеспечивать не требуется.

Требования закона «О персональных данных» вынуждают оператора описать цели обработки, сроки согласия, перечень персональных данных и действия с ними в не только рамках своей организации, но также описать

порядок распространения персональных данных с упоминанием возможных контрагентов. Но, бизнес процессы меняются, меняются информационные технологии и контрагенты. Вывод – надо упрощать соглашение о конфиденциальности.

Исходя из вышесказанного, предлагается такое соглашение:

«*Я (ФИО полностью), паспорт (иной документ, удостоверяющий личность) серия___№____, выдан (кем и когда), настоящим подтверждаю свое согласие на обработку и использование моих персональных данных (наименование и адрес компании) в целях заключения и реализации Договора. При этом все передаваемые мною персональные данные в рамках Договора согласен считать общедоступными персональными данными до отзыва согласия посредством письменного заявления.*»

В случае такого заявления защита персональных данных, в соответствие с требованиями закона «О персональных данных», также не требуется.

При этом надо различать общедоступность информации, к которой предоставлен доступ неограниченного круга лиц, с распространением персональных данных.

Общедоступность не означает обязательное ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

Общедоступность признается только в отношении передаваемых персональных данных и только для данной организации. При заключении договора с другой организацией субъект может установить другой режим персональных данных – режим конфиденциальности персональных данных.

Согласие считать персональные данные общедоступными означает только то, что субъект персональных данных согласен с передоверием оператору возможности регулирования доступа к его персональным данным.

Можно ли доверять оператору? С точки зрения бизнеса все телефоны клиентов и иная информация о клиенте относится к коммерческой тайне, и бизнес заинтересован в выполнении закона №98-ФЗ «О коммерческой тайне», который вводит понятия коммерческая тайна и режим конфиденциальности информации.

К информации, составляющей коммерческую тайну, относятся сведения любого характера, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны. В соответствии ст.5 закона «О коммерческой тайне» персональные данные не относятся к сведениям, которые не могут составлять коммерческую тайну. Следовательно, оператор на основе Федерального закона №98-ФЗ «О коммерческой тайне» может ввести режим

коммерческой тайны с запретом на распространение персональных данных. Кроме того, воля субъекта передать право распоряжаться доступом к его персональным данным для неограниченного круга лиц, может относиться к информации, составляющую коммерческую тайну. То есть, как договор страхования, так и соглашение об общедоступности персональных данных могут относиться к информации, составляющую коммерческую тайну.

Наказание за разглашение коммерческой тайны более значимое. За разглашение коммерческой тайны работник может быть привлечен к дисциплинарной, административной, гражданско-правовой или уголовной ответственности. Ст. 183 УК РФ, карающей за "незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну", определяет и меру наказания - лишение свободы на срок до десяти лет.

Заключение

Проблема защиты персональных данных лежит не только в плоскости организаций - операторов персональных данных, но и напрямую зависит от интересов самих субъектов персональных данных. Закон позволяет учесть эти интересы и упростить взаимоотношения субъекта с оператором.

Для достижения этой цели:

1.Необходимо пересмотреть соглашение о конфиденциальности, заключаемое с субъектом персональных данных, в сторону общедоступности данных о субъекте.

2.Необходимо шире использовать способы обезличивания персональных данных.

3.Необходимо вывести коммерческие организации из-под действия закона «О персональных данных», так как есть более действенный закон «О коммерческой тайне».

4.Необходимо ужесточить неправомерное использование (утечки) персональных данных в государственных организациях.

5.Необходимо наладить легитимное информационное взаимодействие между коммерческими и государственными организациями по обмену персональными данными с целью обеспечения безопасности, противодействия мошенничеству.

СПИСОК ЛИТЕРАТУРЫ

1. Федеральный закон № 152-ФЗ «О персональных данных» от 27.02.2006.
2. Петров М. И. Комментарий к Федеральному закону «О персональных данных» (постатейный). – М.: Юстицинформ, 2007.
3. Рябко С. Об обезличивании персональных данных, http://www.itsec.ru/articles2/focus/ob-obezlichivanii-personaljnyh-dannyh.
4. Кучин И.Ю. Защита конфиденциальности персональных данных с помощью обезличивания ISSN 2072-9502 Вестник АГПУ.Сер.: Управление, вычислительная техника и информатика. 2010.№2.

5. k-Anonymity / V. Ciriani, S. De Capitani di Vimercati, S. Foresti, P. Samarati // Springer US, Advances in Information Security. – 2007.
6. Саксонов Е.А., Щередин Р.В. Процедура обезличивания персональных данных Московский государственный институт электроники и математики (МИЭМ) Наука и образование Электронное научно-техническое издание, март 2011, http://technomag.edu.ru/doc/173146.html.
7. Методика обезличивания персональных данных. Патент компании ООО «Стратегия безопасности» на http://www.bio5.ru/news/obezlichivanie-personalnyh-dannyh.html.