МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФГБОУ ВО
«БРЯНСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра «Системы информационной безопасности»

«ТРАНСГРАНИЧНАЯ ПЕРЕДАЧА ПЕРСОНАЛЬНЫХ ДАННЫХ»

Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 31.12.2017) "О персональных данных"

Статья 12. Трансграничная передача персональных данных

1. Трансграничная передача персональных данных на территории иностранных государств, являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, а также иных иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных, осуществляется в соответствии с настоящим Федеральным законом и может быть запрещена или ограничена в целях защиты основ конституционного строя Российской Федерации, нравственности, здоровья, прав и законных интересов граждан, обеспечения обороны страны и безопасности государства.

2. Уполномоченный орган по защите прав субъектов персональных данных утверждает перечень иностранных государств, не являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных и обеспечивающих адекватную защиту прав субъектов персональных данных. Государство, не являющееся стороной Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, может быть включено в перечень иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных, при условии соответствия положениям указанной Конвенции действующих в соответствующем государстве норм права и применяемых мер безопасности персональных данных.

3. Оператор обязан убедиться в том, что иностранным государством, на территорию которого осуществляется передача персональных данных, обеспечивается адекватная защита прав субъектов персональных данных, до начала осуществления трансграничной передачи персональных данных.

4. Трансграничная передача персональных данных на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных, может осуществляться в случаях:

1) наличия согласия в письменной форме субъекта персональных данных на трансграничную передачу его персональных данных,

2) предусмотренных международными договорами Российской Федерации,

3) предусмотренных федеральными законами, если это необходимо в целях защиты основ конституционного строя Российской Федерации, обеспечения обороны страны и безопасности государства, а также обеспечения безопасности

устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства,

4) исполнения договора, стороной которого является субъект персональных данных,

5) защиты жизни, здоровья, иных жизненно важных интересов субъекта персональных данных или других лиц при невозможности получения согласия в письменной форме субъекта персональных данных.

"Конвенция о защите физических лиц при автоматизированной обработке персональных данных"
(Заключена в г. Страсбурге 28.01.1981) (вместе с Поправками к Конвенции о защите физических лиц при автоматизированной обработке персональных данных (СДСЕ N 108), позволяющими присоединение европейских сообществ, принятыми Комитетом Министров в Страсбурге 15.06.1999)

Цель настоящей Конвенции состоит в обеспечении на территории каждой Стороны для каждого физического лица, независимо от его гражданства или местожительства, уважения его прав и основных свобод, и в частности его права на неприкосновенность частной жизни, в отношении автоматизированной обработки касающихся его персональных данных ("защита данных").

Стороны обязуются применять настоящую Конвенцию в отношении автоматизированных файлов персональных данных и автоматизированной обработки персональных данных в государственной и частной сферах.

Любое государство, расширившее сферу применения настоящей Конвенции путем любого из заявлений, предусмотренных в подпунктах b) или c) пункта 2 выше, может уведомить с помощью указанного заявления о том, что такое расширение касается лишь определенных категорий файлов персональных данных, перечень которых будет сдан на хранение.

Никакая Сторона, исключившая определенные категории автоматизированных файлов персональных данных путем заявления, предусмотренного в подпункте a) пункта 2 выше, не может требовать применения настоящей Конвенции в отношении таких категорий от Стороны, которая их не исключила.

Персональные данные, подвергающиеся автоматизированной обработке:

a) собираются и обрабатываются на справедливой и законной основе,

b) хранятся для определенных и законных целей и не используются иным образом, несовместимым с этими целями,

c) являются адекватными, относящимися к делу и не чрезмерными для целей их хранения,

d) являются точными и, когда это необходимо, обновляются,

e) сохраняются в форме, позволяющей идентифицировать субъекты данных, не дольше, чем это требуется для целей хранения этих данных.

Персональные данные, касающиеся расовой принадлежности, политических взглядов или религиозных или других убеждений, а также персональные данные, касающиеся здоровья или половой жизни, не могут подвергаться

автоматизированной обработке, если внутреннее законодательство не устанавливает соответствующих гарантий. Это положение действует также в отношении персональных данных, касающихся судимости.

Любому лицу должна быть предоставлена возможность:

a) знать о существовании автоматизированного файла персональных данных, знать его основные цели, а также название и место обычного проживания или местонахождение контролера файла,

b) получить через разумный промежуток времени и без чрезмерной задержки или чрезмерных расходов подтверждение того, хранятся ли касающиеся его персональные данные в автоматизированном файле данных, а также получить такие данные в доступной для понимания форме,

c) добиваться в случае необходимости исправления или уничтожения таких данных, если они подвергались обработке в нарушение норм внутреннего законодательства, воплощающего основополагающие принципы, изложенные в Статьях 5 и 6 настоящей Конвенции,

d) прибегать к средствам правовой защиты в случае невыполнения просьбы о подтверждении или в случае необходимости предоставлении данных, их изменении или уничтожении, как это предусмотрено в пунктах b) и c) настоящей Статьи.

Каждая Сторона обязуется предусмотреть надлежащие санкции и средства правовой защиты на случай нарушения норм внутреннего законодательства, воплощающих основополагающие принципы защиты данных.

Никакие положения настоящей Главы не должны толковаться как ограничивающие или иным образом ущемляющие возможность Стороны обеспечить субъектам данных большую степень защиты, чем та, которая предусмотрена настоящей Конвенцией.

Сторона не должна запрещать или обусловливать специальным разрешением трансграничные потоки персональных данных, идущие на территорию другой Стороны, с единственной целью защиты частной жизни.

Тем не менее каждая Сторона вправе отступать от положений пункта:

a) в той степени, в какой ее внутреннее законодательство включает специальные правила в отношении определенных категорий персональных данных или автоматизированных файлов персональных данных в силу характера этих данных или этих файлов, за исключением случаев, когда правила другой Стороны предусматривают такую же защиту,

b) когда передача осуществляется с ее территории на территорию государства, не являющегося Стороной настоящей Конвенции, через территорию другой Стороны, в целях недопущения такой передачи, которая позволит обойти законодательство Стороны, упомянутой в начале данного пункта.

Каждая Сторона оказывает помощь любому лицу, постоянно проживающему за границей, в осуществлении прав, предоставленных нормами ее внутреннего законодательства, воплощающими принципы, изложенные в Статье 8 настоящей Конвенции.

Каждая Сторона следит за тем, чтобы лица, работающие в назначенном органе или действующие от его имени, были связаны надлежащими обязательствами сохранять секретность или конфиденциальность этой информации.

Каждая Сторона назначает в Комитет представителя и заместителя представителя. Любое государство - член Совета Европы, не являющееся Стороной Конвенции, имеет право быть представленным в Комитете наблюдателем.

ПРИКАЗ от 15 марта 2013 г. N 274 «ОБ УТВЕРЖДЕНИИ ПЕРЕЧНЯ ИНОСТРАННЫХ ГОСУДАРСТВ, НЕ ЯВЛЯЮЩИХСЯ СТОРОНАМИ КОНВЕНЦИИ СОВЕТА ЕВРОПЫ О ЗАЩИТЕ ФИЗИЧЕСКИХ ЛИЦ ПРИ АВТОМАТИЗИРОВАННОЙ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ И ОБЕСПЕЧИВАЮЩИХ АДЕКВАТНУЮ ЗАЩИТУ ПРАВ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ»

В данный перечень включены следующие страны:

Австралия - Австралийский союз, Аргентинская Республика, Габонская Республика, Государство Израиль, Государство Катар, Канада, Королевство Марокко, Малайзия, Мексиканские Соединенные Штаты, Монголия, Новая Зеландия, Республика Ангола, Республика Бенин, Республика Кабо-Верде, Республика Казахстан, Республика Коста-Рика, Республика Корея, Республика Мали, Республика Перу, Республика Сингапур, Тунисская Республика, Республика Чили, Южно-Африканская Республика.

Трансграничная передача в КНР.
Защита ПДн в КНР.

Конституция КНР гарантирует защиту достоинства личности и тайну переписки. Положения о защите ПД содержатся в отдельных нормативно-правовых актах.

05 ноября 2012 года было принято «Руководство по защите персональной информации в информационной системе по оказанию публичных и коммерческих услуг», в котором было дано следующее определение:

Персональные данные — любая информацию об определенном физическом лице, которая сама по себе или в комбинации с другой информацией позволяет его идентифицировать.

Руководство устанавливает обязанность оператора ПДн получать согласие субъекта ПДн на обработку и сообщать ему о цели обработки, сроке хранения, мерах по защите ПДн и так далее.
О локализации ПДн, то о ней говорится в ст.5.4.5:

При отсутствии ясно выраженного согласия субъекта ПДн, нормативного разрешения или согласия уполномоченных органов оператор ПДн не должен передавать ПДн какому-либо лицу, находящемуся за рубежом, включая любых физических лиц, проживающих за рубежом, или любых организаций и компаний, которые зарегистрированы за рубежом.

Так же, о персональных данных говорится и в принятом 25.10.2013 законе о защите потребителей:

Статья 29. При сборе и использовании персональных данных физических лиц участники предпринимательской деятельности обязаны следовать принципам законности, обоснованности и необходимости, явным образом информировать о цели, способах и пределах сбора и использования информации и получить согласие потребителя.

Субъекты предпринимательской деятельности обязаны предпринимать технические и другие необходимые меры для обеспечения безопасности информации и предотвращения раскрытия или утечки ПДн потребителей.

Кроме того, есть еще ряд НПА, тем или иным образом затрагивающие защиту субъектов ПДн.

Закон КНР «О деликатной ответственности» 2009 года, защищающий право на неприкосновенность частной жизни и, в частности, предусматривает ответственность медицинского учреждения за распространение ПДн без согласия субъекта ПДн.

«Решение об усилении защиты информации в Интернете», принятое Парламентом КНР 28.12.2012

«Положение об электросвязи и защите персональной информации интернет-пользователей», принятое 19.07.2013

15 марта 2015 года вступили в силу «Меры ответственности за нарушения прав и интересов потребителей», разработанные и принятые Государственным управлением по промышленности и коммерции Китая (SAIC).

Последний указанный акт представляет особый интерес в отношении определения персональных данных в контексте защиты прав потребителя. Согласно Мерам, к ПДн потребителя относятся следующие данные: имя, пол, профессия, дата рождения, номер паспорта, адрес, контактная информация, сведения о доходах и собственности, сведения о здоровье, привычки потребителя.

1 июня 2017 года вступил в силу «Закон о кибербезопасности». Закон о кибербезопасности является первым сводным законом, регулирующим практически все проблемы данной сферы в Китае. В том числе, он, конечно же, касается и ПДн.

Хранение личных данных и других важных данных должно обеспечиваться исключительно на территории КНР (статья 37).

Закон о кибербезопасности подтверждает обязанности сетевых операторов в отношении защиты персональной информации, которые определены существующим законодательством и регуляторными требованиями, включая право на отслеживание соблюдения принципа законности, необходимости и уместности сбора и использования личных данных, а также право наблюдения за выполнением «требований об информировании и получении согласия» (статья 41) об использовании личных данных лишь в тех целях на которые дало согласие соответствующее лицо (статья 41), право принимать меры защиты безопасности личных данных (статья 42) и защищать индивидуальное право оценивать и вносить исправления в личную информацию (статья 43).

Кроме того, Закон о кибербезопасности также включает в себя некоторые новые правила в отношении защиты личных данных, включая требования об уведомлении о нарушении защиты данных (статья 42), об анонимизации данных в качестве исключения в требованиях об информировании и получении согласия (статья 42), а также об праве индивида требовать у сетевых операторов внести изменения в или удалить его личные данные в случае, если информация о нём ошибочна или используется в несогласованных с ним целях (статья 43).

Трансграничная передача в США

В Соединенных Штатах Америки до сих пор отсутствует общее (федеральное) законодательство о персональных данных. В случае же нарушения прав субъектов персональных данных применяются положения Конституции и практика прецедентного права, преобладающего в США.

В США, как и во многих других странах мира, сложилась собственная практика защиты конфиденциальной информации, которая характеризуется наличием закона о частной жизни и уполномоченными по защите частной жизни. Известно, что общее законодательство в Соединенных Штатах, в большинстве своем, направлено на регулирование деятельности государственных органов, входящих в структуру исполнительной власти, с целью создания прозрачного механизма управления и подотчетности обществу.

Это в полной мере относится к сфере обработки персональных данных, где основными действующими документами являются Privacy Act of 1974 и Privacy Protection Act of 1980, регулирующие деятельность органов государственной власти при обработке персональных данных граждан. Однако, упомянутые нормативные акты, не всегда отвечают стремительно меняющимся условиям современного мира, характеризующегося международной интеграцией и колоссальным прогрессом в области информационных технологий.

Ещё одной из отличительных черт защиты данных в США является, так называемый «зонтичный» подход, обеспечивающий адекватную защиту данных в отдельных областях (при исполнении отдельных договоров), который основан на использовании общего законодательства, отраслевых подзаконных актов и рекомендаций по защите информации, выраженных в т.ч. в примерах договоров. Примером такого «зонтичного» соглашения служит US Department of Commerce's Safe Harbor Privacy Principles (Принципы защиты информации Министерства торговли США) и Transfer of Air Passenger Name Record (PNR) Data (передача данных таможне и пограничной службе США) где, по заключению Еврокомиссии, обеспечивается адекватная защита данных.

В качестве рекомендаций по обеспечению защиты данных широко применяются документы «Дирекции управления и бюджета» (OMB — Office of Management and Budget) и «Национального института стандартов и технологий» (NIST - National Institute of Standards and Technology). Указанные нормативные акты регулируют деятельность по защите персональных данных в государственных структурах, для коммерческих же организаций они носят рекомендательный характер. В качестве борьбы с утечками конфиденциальной информации был задействован следующий механизм: каждый штат принимает закон, обязывающий компании сообщать о любых утечках информации.

Очередным шагом к централизованному регулированию отношений, связанных с обработкой персональных данных граждан, является документ NIST Special Publication 800-122 Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) (Draft), проект которого вышел в свет в январе 2009 года. Цель документа - помощь государственным организациям и федеральным агентствам в защите персональных данных граждан.

NIST Special Publication 800-122 содержит общие рекомендации по защите персональных данных и ссылается на многочисленные нормативно-правовые акты внутреннего законодательства США, в которых отражены различные организационные, технические, юридические аспекты защиты ПДн.

Рекомендации по обеспечению защиты персональных данных в организации по версии NIST Special Publication 800-122 рассматривают темы:

Проведение обследования с целью: выявления обрабатываемых ПДн. определение категорий ПДн по уровню потенциального ущерба. установления круга лиц, имеющих доступ к ПДн и др.

Общие меры защиты ПДн: создание в организации политик и процедур обработки ПДн (контроль доступа к ПДн, правила хранения ПДн, правила передачи третьим лицам, реагирование на инциденты безопасности и др.).

Обучение, повышение информированности сотрудников (план проведения обучения сотрудников правилам обработки ПДн).

Дополнительные меры защиты: уменьшение объемов обрабатываемых и хранимых ПДн (удаление ПДн по достижению целей их обработки), обезличивание ПДн (деление ПДн на части. добавление «шума» (посторонней информации) в ПДн для усложнения идентификации ПДн. группирование общих характеристик ПДн. скрытие части данных и др.).

Обеспечение безопасности ПДн: управление доступом к ПДн. разделение прав доступа (все пользователи работают с обезличенной информацией, к кодам имеют доступ ограниченный круг пользователей). уменьшение количества привилегированных пользователей. запрет или ограничение на удаленный доступ. запрет или ограничение на хранение и обработку ПДн на мобильных устройствах. контроль попыток несанкционированного доступа к ПДн. мониторинг, анализ, уведомление (анализ активности пользователей в отношении ПДн). авторизация пользователей для доступа к ПДн. ограничение возможности копирования ПДн на внешние носители. шифрование ПДн, передаваемых за пределы организации и др.

Ответственность за нарушение правил трансграничной передачи данных

В отношении субъектов, нарушающих правила о локализации могут быть предусмотрены следующие санкции:

1. Ст.13.11 КОАП РФ устанавливает штраф за нарушение порядка сбора, хранения, использования или распространения персональных данных. Влечет предупреждение или наложение административного штрафа на граждан в размере от одной тысячи до трех тысяч рублей. на должностных лиц - от пяти тысяч до десяти тысяч рублей. на юридических лиц - от тридцати тысяч до пятидесяти тысяч рублей.
2. В качестве другой санкции может быть применена возможность внесения доменных имен и сетевых адресов в реестр нарушителей прав субъектов персональных данных.

Если перед тем как будет осуществлена трансграничная передача персональных данных, своевременно не уведомить Роскомнадзор, то данное бездействие будет носить характер незаконного деяния. Такое правонарушение попадает под ст. 19.6 КоАП (Непринятие мер по устранению причин и условий, способствовавших совершению административного правонарушения) . Влечет наложение административного штрафа на должностных лиц в размере от четырех тысяч до пяти тысяч рублей. Направление сообщения в Роскомнадзор после совершения операции также приравнивается к несоблюдению установленного регламента.

АДЕКВАТНАЯ ЗАЩИТА

Организационная структура компании – ЗАО «Брянск Бизнес Банк»:

1. Руководство
2. Бухгалтерия (обрабатываются данные работников организации, данные лицевых счетов клиентов организации).
3. Отдел кадров (обрабатываются ПДн работников организации).
4. Отдел кассовых операций (данные лицевых счетов клиентов).
5. Юридический отдел (ПДн клиентов организации).
6. Отдел кредитования (ПДн клиентов).
7. Отдел безопасности: администратор информационной безопасности (несет ответственность за НСД к ПДн сотрудников и клиентов, за инструктаж сотрудников, за нормативно-правовую и организационную деятельность в области защиты ПДн), системный администратор (несет ответственность за выход из строя оборудования), охранник (несет ответственность за физический доступ в организацию).
   За разглашение ПДн несет ответственность сотрудник, совершивший нарушение.

Положение о трансграничной передаче ПДн.

Общие положения

1. Термины и определения

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Субъект персональных данных – физическое лицо, прямо или косвенно определенное или определяемое с помощью персональных данных.

Трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

Контролируемая зона – это пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание сотрудников и посетителей организации, а также транспортных средств. Информационная система персональных данных – совокупность, содержащихся в базах данных, персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

2. Цели и сфера действия Положения

Положение об обработке персональных данных (далее – Положение) является основополагающим локальным нормативным актом, определяющим позицию ЗАО «Брянск Бизнес Банк» (далее – Компании) в отношении обработки и обеспечения безопасности персональных данных. Основной целью настоящего Положения является создание основы для соблюдения прав и свобод человека и гражданина при обработке его персональных данных Организацией.

3. Законодательство Российской Федерации в области обработки и обеспечения безопасности персональных данных

Настоящий документ разработан с учетом положений следующих нормативных правовых актов Российской Федерации:

- Конституция Российской Федерации.
- Доктрина информационной безопасности Российской Федерации.
- Федеральный закон от 19.12.2005 №160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных».
- Федеральный закон от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации».
- Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных» (далее – ФЗ №152 «О персональных данных»).
- Трудовой кодекс Российской Федерации.
- Постановление Правительства Российской Федерации от 15.09.2008 №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».
- Постановление Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

4. Основания обработки персональных данных

Обработка персональных данных Компанией осуществляется в следующих случаях:

- с согласия субъекта персональных данных на обработку его персональных данных.
- для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на Компанию функций, полномочий и обязанностей.
- для исполнения договора, стороной которого, либо выгодоприобретателем или поручителем по которому является субъект персональных данных, в том числе в случае реализации оператором своего права на уступку прав (требований) по такому договору, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем.
- для осуществления прав и законных интересов Компании или третьих лиц, либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных.

• при необходимости осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве.
• в случае, если такая обработка необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно.
• в случае, когда доступ неограниченного круга лиц к персональным данным субъекта предоставлен самим субъектом персональных данных, либо по его просьбе (далее – персональные данные, сделанные общедоступными субъектом персональных данных).
• в случае, когда персональные данные подлежат опубликованию или обязательному раскрытию в соответствии с федеральным законом.
• в статистических или иных исследовательских целях, при условии обязательного обезличивания персональных данных.

Компания ЗАО «Брянск Бизнес Банк» зарегистрирована в реестре операторов, осуществляющих обработку персональных данных под номером 32-32-001001 Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, судимости Компанией не осуществляется. Обработка указанных данных возможна Компанией только на основании согласия субъекта персональных данных в письменной форме.

5. Передача персональных данных третьим лицам

Компания при осуществлении своей деятельности может передавать персональные данные субъектов государственным органам (Федеральной налоговой службе, Федеральной службе судебных приставов, Министерству внутренних дел Российской Федерации, Прокуратуре и др.) в рамках осуществления последними своих полномочий и функций, а также контрагентам Компании (банкам, страховым компаниям, коллекторским агентствам и др.) в строгом соответствии с требованиями законодательства Российской Федерации, локальных актов и при надлежащем обеспечении безопасности этих данных.

6. Трансграничная передача персональных данных

Компанией может осуществляться трансграничная передача персональных данных на территории иностранных государств, являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной

обработке персональных данных, а также на территории иностранных государств, приведенных в «Перечне иностранных государств, не являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных и обеспечивающих адекватную защиту прав субъектов персональных данных» (утвержден Приказом Роскомнадзора от 15.03.2013 №274). Трансграничная передача персональных данных на территории иных иностранных государств, может осуществляться в случаях:

- наличия согласия в письменной форме субъекта персональных данных на трансграничную передачу его персональных данных.
- исполнения договора, стороной которого является субъект персональных данных.

1.10 Прекращение обработки и уничтожение персональных данных

Обработка персональных данных прекращается или обеспечивается её прекращение, если обработка персональных данных осуществляется другим лицом, действующим по поручению Компании, а собранные персональные данные уничтожаются1 в сроки, установленные ФЗ №152 «О персональных данных», в следующих случаях, если иное не установлено законодательством Российской Федерации:

- по истечению установленного срока обработки персональных данных.
- по достижении целей обработки или при утрате необходимости в их достижении.
- по требованию субъекта персональных данных или Уполномоченного органа по защите прав субъектов персональных данных — если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки.
- при отзыве субъектом персональных данных согласия на обработку своих персональных данных, если такое согласие требуется в соответствии с федеральным законодательством.
- при невозможности устранения Компанией допущенных нарушений при обработке персональных данных.

7. Ответственность

Ответственность за выполнение требований ФЗ №152 «О персональных данных» в Компании возложена на руководство Компании в лице Генерального директора.

Ответственность за организацию обработки и обеспечения безопасности персональных данных в соответствии с требованиями ФЗ №152 «О персональных данных» и настоящего Положения возложена на структурные подразделения, ответственные за обеспечение безопасности персональных данных.

Персональная ответственность за выполнение требований по обработке и обеспечению безопасности персональных данных возложена на руководителей структурных подразделений и сотрудников Компании, осуществляющих обработку персональных данных.

Сотрудники Компании при нарушении установленного порядка обработки и обеспечения безопасности персональных данных, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством Российской Федерации.

Инструкция пользователю при трансграничной передаче ПДн

1. Уведомить Роскомнадзор об осуществляемой трансграничной передаче.
2. Проинформировать субъекта персональных данных до начала обработки его персональных данных об осуществляемой трансграничной передаче.
3. Отразить условия трансграничной передачи персональных данных во внутренних нормативных документах Организации. Необходимо руководствоваться :
   Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ.
   Федеральный закон от 21.07.2014 № 242-ФЗ.

- Правовое обоснование трансграничной передачи персональных данных (перечень нормативно – правовых документов, на основании которых осуществляется передача и обработка ПДн).
- Регламент обеспечения безопасного обмена ПДн.
- Описание мероприятий и средств обеспечения защиты передаваемых ПДн. (организационные мероприятия. технические средства защиты информации, в том числе средства криптографической защиты информации).

4. Заключить договор с компанией, которой данные передаются, где указать

- перечень действий, осуществляемых с персональными данными.
- цели обработки.
- обязанность обработчика соблюдать конфиденциальность ПДн и обеспечивать безопасность ПДн при их обработке.
- требования к защите обрабатываемых ПДн. При этом, организация, которой передаются ПДн при организации обработки будет руководствоваться законодательством страны пребывания.

5. Обеспечить защиту канала передачи данных

После принятия Федерального закона от 21.07.2014 № 242-ФЗ было введено описанное ранее требование о “локализации” персональных данных.

ЗАО «Брянск Бизнес Банк»

ПРИКАЗ

25.03.2019 г. №101

об утверждении перечня ПДн, передаваемых трансграничным путем (в бумажном виде)

В соответствии с Постановлением Правительства Российской Федерации от 21.03.2012 г. №221 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, ПРИКАЗЫВАЮ :

1. Утвердить прилагаемый Перечень персональных данных, передаваемых трансграничным путем ЗАО ««Брянск Бизнес Банк».

Контроль за исполнением настоящего приказа оставляю за собой.

Руководитель _____ И.И.Иванов

ЗАО «Брянск Бизнес Банк»

ЗАО «Брянск Бизнес Банк»

УТВЕРЖДЕН

Приказом №101

От 25.03.2019 г.

Перечень персональных данных, передаваемых ЗАО «Брянск Бизнес Банк» трансграничным путем

1. Перечень персональных данных, передаваемых ЗАО «Брянск Бизнес Банк» трансграничным путем:
   Фамилия, имя, отчество.
   Дата, место рождения.
   Пол.
   Гражданство.
   Адрес проживания.
   Адрес регистрации.
   Паспортные данные.
   ИНН.
   Страховой номер индивидуального лицевого счёта.
   Телефонный номер.
   Данные лицевого, расчетного счета

ЗАО «Брянск Бизнес Банк»

ПРИКАЗ

25.03.2019 г.

№ 102

об утверждении описании мероприятий и средств обеспечения защиты передаваемых ПДн трансграничным путем

В соответствии с Постановлением Правительства Российской Федерации от 21.03.2012 г. №221 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, ПРИКАЗЫВАЮ выполнить следующие мероприятия:

1. Организационные мероприятия:
   1. Определение круга лиц, допущенного к обработке персональных данных.
   2. Организация доступа в помещения, где осуществляется обработка ПДн.
   3. Разработка должностных инструкций по работе с персональными данными.
   4. Установление персональной ответственности за нарушения правил обработки ПДн.
   5. Определение продолжительности хранения ПДн и т.д.
   6. Разработка организационно-распорядительной документации:
      - план мероприятий по обеспечению защиты ПДн;
      - план проверок состояния ИСПДн;
      - инструкция администратора безопасности ИСПДн;
      - перечень персональных данных, передаваемых ЗАО «Брянск Бизнес Банк» трансграничным путем;
      - инструкция пользователю при трансграничной передаче ПДн;

- положение об обработке персональных данных;
- положение по защите персональных данных;
- регламент взаимодействия с субъектами персональных данных;
- регламент взаимодействия при передаче персональных данных третьим лицам.

2. Программно-аппаратные мероприятия:
   1. Установка средств идентификации и аутентификации пользователей ИСПДн.
   2. Установка средств разграничения доступа.
   3. Установка средств регистрации событий безопасности.
   4. Установка криптографических средств защиты информации.
   5. Установка межсетевых экранов.
   6. Установка средств антивирусной защиты.
3. Технические мероприятия:
   1. Получение лицензии на выполнение такого вида деятельности.
   2. Тщательное обследование информационных ресурсов предприятия в соответствии с методическими рекомендациями ФСТЭК (определение перечня ПДн, подлежащих защите.
   3. Определение состава и структуры каждой информационной системы ПДн (ИСПДн).
   4. Анализ уязвимых звеньев и возможных угроз безопасности ПДн.
   5. Оценка ущерба от реализации угроз безопасности ПДн.
   6. Анализ имеющихся в распоряжении мер и средств защиты ПДн.
   7. На основании проведенного обследования осуществляется обоснование требований по обеспечению безопасности ПДн (разработка модели угроз и модели нарушителя безопасности ПДн.
   8. Определение класса информационных систем ПДн.
   9. При необходимости обосновывается использование средств шифрования).
   10. Работы по проектированию, созданию и вводу в эксплуатацию системы защиты ПДн (разработка перечня мероприятий по защите ПДн в соответствии с выбранным классом ИСПДн. согласование документов с регуляторами).

11. Разработка технического задания на создание системы защиты ПДн.
12. Развертывание и ввод в эксплуатацию системы защиты ПДн).
13. Аттестация (сертификация) информационных систем ПДн по требованиям безопасности информации.
14. Сертификация средств защиты информации, работы по аттестации (сертификации) выполняются при наличии соответствующих лицензий.

4. Мероприятия по физической защите:
установка сигнализации.
установка КПП.
установка шумоизолирующих дверей и окон.
установка решеток на окна.
установка жалюзи.

Контроль за исполнением настоящего приказа оставляю за собой.

Руководитель
ЗАО «Брянск Бизнес Банк» _____ И.И.Иванов

Состав законодательства Финляндии в области защиты ПДн

Основным законом, отражающим вопросы защиты ПДн в Финляндии является Закон Финляндии 523/1999 «О персональных данных» (Henkilötietolaki 1999/523).

В нем ответственностью за нарушение для юридических лиц предусматривается возмещение экономического и иного ущерба, понесенного субъектом данных или иным лицом вследствие обработки ПДн в нарушение положений законодательства.

Финляндия входит в число стран, подписавших и ратифицировавших конвенцию о защите физических лиц при автоматизированной обработке персональных данных.

Правила в сфере защиты персональных данных, применимые на территории Финляндии, стали значительно жёстче с принятием Общего регламента о защите данных (General Data Protection Regulation, GDPR; 679/2016), вступившего в силу в мае 2018 года после двухлетнего переходного периода.

GDPR применяется к процессу обработки персональных данных внутри ЕС, но дополнительно он устанавливает требование, что иностранные компании, обрабатывающие персональные данные граждан ЕС, соблюдают правила, определённые Регламентом. Обработка персональных данных на практике включает в себя любые действия с персональными данными, такие как сбор, использование, хранение, передачу, удаление или исправление персональных данных.

GDPR определяет основные принципы обработки персональных данных, то есть защиту данных по конструкции и защиту данных по умолчанию. Защита данных по умолчанию означает, что компания должна принять соответствующие технические и организационные меры для обеспечения того, что обработке подлежат только персональные данные, необходимые для достижения конкретной цели. В то же время, под защитой данных по конструкции понимается обязанность компании принять соответствующие технические и организационные меры для защиты персональных данных, которые она обрабатывает.

Персональные данные могут обрабатываться компанией только тогда, когда она имеет юридические основания для обработки рассматриваемых персональных данных. Обычно такие основания имеются в случае заключения с физическим лицом договора, исполнение которого требует обработки персональных данных указанного лица.

GDPR устанавливает санкции на сумму до 20 миллионов евро для компаний, которые не соблюдают правила, установленные GDPR. Таким образом, компаниям рекомендуется убедиться, что их деятельность по обработке персональных данных осуществляется в соответствии с Регламентом.

Согласие на трансграничную передачу ПДн

СОГЛАСИЕ

на трансграничную передачу персональных данных

Я, _____, зарегистрированный (ая) по адресу:

_____,

Паспорт ___ №_____, выдан_____,

даю письменное согласие на обработку (в том числе трансграничную передачу) моих персональных данных, а именно :

1. _____
2. _____

Данное согласие предоставляю _____.

Фамилия, инициалы (подпись) (дата)

Защита ПДн в Азербайджане

ЗАКОН АЗЕРБАЙДЖАНСКОЙ РЕСПУБЛИКИ

О персональных данных
от 11 мая 2010 года №998-IIIQ
Органы эмитенты:Парламент
(В редакции Законов Азербайджанской Республики от 20.06.2014 г. №995-IVQD, 03.04.2018 г. №1066-VQD)

Настоящий Закон регулирует отношения, связанные со сбором, обработкой и защитой персональных данных, формирование раздела персональных данных в национальном информационном пространстве, а также вопросы, связанные с трансграничной передачей персональных данных, устанавливает права и обязанности действующих в данной сфере государственных органов и органов местного самоуправления, физических и юридических лиц.

Законодательство Азербайджанской Республики в сфере персональных данных состоит из Конституции Азербайджанской Республики, международных договоров, участницей которых является Азербайджанская Республика и настоящего Закона.

В целях обеспечения национальной безопасности Азербайджанской Республики, а также законности правила сбора персональных данных в связи с осуществлением разведывательной и контрразведывательной, оперативно-розыскной деятельности, защиты персональных данных, относящихся к государственной тайне и собранных в национальном архивном фонде, устанавливаются соответствующим законодательством Азербайджанской Республики.

Положения настоящего Закона не распространяются на сбор и обработку персональных данных физическими лицами исключительно для личных и семейных нужд.

Статья 1. Цель ЗаконаОсновная цель настоящего Закона состоит в определении законодательных основ и общих принципов сбора, обработки и защиты персональных данных, правил и требований государственного регулирования в данной сфере, правил формирования персональных данных в информационных ресурсах, создания информационных систем, предоставления и передачи информации, прав, обязанностей и основ ответственности участвующих в данном процессе лиц, защите основных прав и свобод человека и гражданина, в том числе права на сохранение тайны личной и семейной жизни

Статья 14. Трансграничная передача персональных данных

14.1. Трансграничная передача персональных данных осуществляется при соблюдении установленных настоящим Законом требований и с учетом установленных настоящей статьей особенностей.

14.2. Трансграничная передача персональных данных запрещается в следующих случаях:

14.2.1. при наличии угрозы для национальной безопасности Азербайджанской Республики;

14.2.2. если законодательство страны, в которую передаются персональные данные, не обеспечивает правовую защиту этих данных на уровне, установленном законодательством Азербайджанской Республики.

14.3. Трансграничная передача персональных данных может осуществляться независимо от уровня их правовой защиты в случаях, когда субъект дал согласие на трансграничную передачу персональных данных, а также если передача персональных данных необходима для охраны жизни и здоровья субъекта.

14.4. При трансграничной передаче персональных данных безопасность этих данных обеспечивается собственником или оператором

Статья 11. Особенности сбора персональных данных

11.1. Собственник или оператор вправе получать от субъекта только те персональные данные, которые необходимы для достижения целей обработки.

11.2. При сборе персональных данных собственник или оператор должен в обязательном порядке сообщить субъекту о следующем:

11.2.1. данные, определяющие собственника или оператора;

11.2.2. цель обработки персональных данных и юридическое обоснование данной цели;

11.2.3. уровень защиты собираемых и обрабатываемых персональных данных в информационной системе;

11.2.4. сведения о наличии сертификата соответствия на информационные системы и о прохождении ими государственной экспертизы;

11.2.5. круг предусмотренных пользователей персональных данных, в том числе информационных систем, с которыми предусмотрено осуществление информационного обмена;

11.2.6. информация об установленных настоящим Законом правах субъекта.

11.3. В случае если предоставление персональных данных установлено законом, собственник или оператор должны проинформировать субъекта о правовых последствиях принудительного предоставления персональных данных. [5]

СУДЕБНОЕ ДЕЛО ПО ТРАНСГРАНИЧНОЙ ПЕРЕДАЧЕ ДАННЫХ

М******* Г.Н. обратилась в суд с иском к АО «*******» о предоставлении информации, касающейся обработки персональных данных, компенсации морального вреда в размере 20 000 руб., взыскании расходов на представителя в размере 5 000 руб. и государственной пошлины в размере 300 руб.

5 июня 2015 г. истец направила в адрес Банка заявление о предоставлении информации, касающейся обработки персональных данных, предоставленных в рамках Договора о выпуске и обслуживании кредитной карты, а именно: подтвердить факт обработки персональных данных, сообщить правовые основания и цели обработки персональных данных, сообщить наименование и сведения о лицах, которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с АО «*******», сообщить наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению АО «*******».

До настоящего времени запрашиваемая информация истцу не предоставлена, что нарушает права истца.

Незаконными действиями банка истцу причинен моральный вред, который она оценивает в 20 000 руб.

При заключении Договора кредитной карты в Заявлении-анкете, истец выразила свое согласие на обработку всех своих персональных данных Банком любыми способами, в том числе третьими лицами, включая осуществление сбора, систематизацию, накопление, хранение, обновление, уточнение (проверка), изменение, использование и распространение (включая передачу), в том числе воспроизведение, электронное копирование и трансграничную передачу … с целью выпуска, обслуживания кредитных карт, для создания информационных систем персональных данных Банка, в целях предоставления информации третьим лицам, которые по договору с Банком осуществляют деятельность по обеспечению погашения должниками просроченной задолженности.

Таким образом, Банк при заключении Договора получил согласие истца на обработку персональных данных в соответствии с требованием вышеуказанного Федерального закона «О персональных данных».

******* 2015 г. истец обратилась в Банк с требованием предоставить информацию, касающуюся обработки персональных данных.

Банк в соответствии со ст. 20 Федерального закона «О персональных данных» ******* 2015 г. направил истцу ответ на заявление от ******* 2015 г.

При таких обстоятельствах, учитывая, что Банк дал ответ на заявление истца, права М******* Г.Н. не нарушены.

Кроме того, истец в силу ст. 56 ГПК РФ не представила суду доказательств, подтверждающих факт нарушения Банком порядка обработки ее персональных данных.

Суд также учитывает, что требования М******* Г.Н. об обязании предоставить ей информацию о лицах, допущенных к обработке ее персональных данных, включая фамилию, имя, отчество и адрес не основаны на положениях ч. 7 ст. 14 Федерального закона «О персональных данных».

Учитывая, что банком не допущено нарушения прав истца как потребителя и заемщика, морально-нравственные страдания М******* Г.Н. причинены не были, порядок обработки персональных данных истца Банком не нарушался, оснований для компенсации морального вреда не имеется.

В удовлетворении иска М******* Г******* Н******* к АО «*******» о предоставлении информации, компенсации морального вреда и судебных расходов - отказать.

СОГЛАСИЕ НА ТРАНСГРАНИЧНУЮ ПЕРЕДАЧУ ДАННЫХ

Я, _____ , зарегистрированный(ая) по адресу:
(ФИО субъекта персональных данных)

_____ ,
(Адрес места постоянной регистрации, номер контактного телефона)

паспорт серии _____ № _____ , выданный _____
_____ "___" _____ 20__ г.
(Наименование органа, выдавшего паспорт) (Дата выдачи паспорта)

даю своей волей письменное согласие на обработку (в том числе трансграничную передачу) моих персональных данных.

Данное согласие предоставляется _____.

Цель обработки персональных данных:

_____

_____.

Перечень персональных данных, на обработку которых дается согласие

1. Фамилия, имя, отчество. Дата и место рождения. Адрес места постоянной и временной регистрации, места фактического проживания. Номер домашнего, мобильного и контактного телефона. Адрес электронной почты. Данные национального и заграничного паспорта.
2. Другие сведения необходимые для достижения указанных целей.

Перечень действий с персональными данными, на совершение которых дается согласие: Трансграничная передача. Сбор. Запись. Систематизация. Накопление. Хранение. Уточнение (обновление, изменение). Извлечение.

Использование. Передача (распространение, предоставление, доступ). Обезличивание. Блокирование. Удаление. Уничтожение.

Общее описание способов обработки персональных данных:

1. Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники.
2. Ручная обработка персональных данных - обработка персональных данных без использования средств вычислительной техники.

Срок, в течение которого действует настоящее согласие: с настоящего момента и до истечения сроков, установленных действующим законодательством Российской Федерации.

Способ отзыва настоящего согласия: Настоящее согласие может быть отозвано на основании письменного заявления субъекта персональных данных.

Субъект персональных данных:

_____ _____

(Подпись) (Фамилия и инициалы)

"___" _____ 20__ г.

(Дата подписи)

Закон о персональных данных в Турции

Согласно новому законопроекту, личные данные не могут быть использованы без прямого согласия их владельца, а также в тех случаях, когда интересам вышеупомянутых лиц может быть нанесен серьезный ущерб. Кроме того, персональные данные могут передаваться представителям других стран только с разрешения новообразованного Совета по защите неприкосновенности персональных данных.

Принятый закон определил в разряд «персональных данных особого свойства» расу, национальность, политические взгляды, философские убеждения, вероисповедание, а также другие убеждения частных лиц, особенности внешности, принадлежность к какой-либо ассоциации, фонду или синдикату, состояние здоровья, информацию о частной жизни и уголовном прошлом, а также биометрические и генетические данные.

Законопроект также дает физическим лицам право знать, что их персональные данные находятся в обработке. Кроме того, в случае, если в процессе обработки информации личного характера была допущена какая-либо ошибка или утечка данных, физические лица имеют право потребовать ее коррекции или удаления. Если граждане понесут какой-либо урон, связанный с незаконной обработкой их персональных данных, они будут вправе потребовать возмещения ущерба.

Судебный случай по тематике «Трансграничная передача ПДн»

Суть спора: истец (Роскомнадзор) обратился в Московский городской суд с требованием признать деятельность интернет-ресурсов (http://www.linkedin.com, http://linkedin.com) по сбору, использованию и хранению персональных данных граждан Российской Федерации нарушающей требования Закона о персональных данных и права граждан на неприкосновенность частной жизни, личную и семейную тайну. По мнению истца, нарушение ответчиком (LinkedIn Corporation) Закона о персональных данных заключалось в сборе персональных данных граждан Российской Федерации без локализации баз данных как того требует Закон о персональных данных. Кроме того, истец через указанные интернет-ресурсы получал доступ к сведениям третьих лиц, не являющимися пользователями LinkedIn, посредством синхронизации с электронной почтой и устройствами пользователей.

Несмотря на то, что ответчик зарегистрирован за пределами Российской Федерации, Роскомнадзор в ходе рассмотрения дела указал на то, что интернет-ресурс направлен на территорию Российской Федерации. Об этом, по мнению Роскомнадзора, свидетельствует наличие русскоязычной версии сайта, а также возможность использования рекламы на русском языке. Отметим, что подобные выводы коррелируются с разъяснениями Министерства связи и массовых коммуникаций Российской Федерации "Обработка и хранение персональных данных в РФ. Изменения с 1 сентября 2015 года".

Исход дела: суд полностью удовлетворил требования истца.

Состав законодательства Японии, отражающего вопросы защиты ПДн

Закон 1989 года об обрабатываемых компьютерами персональных данных, хранимых административными органами, изначально разрабатывался в соответствии с Руководящими принципами ОЭСР и предусматривает защиту персональных данных, которые обрабатываются с использованием компьютеров, принадлежащих административным органам правительства страны.

Региональный орган по защите данных является местная комиссия по защите неприкосновенности частной жизни.

Так как вышеупомянутый закон 1989 года охватывает только органы центрального правительства. Меры административного регулирования ограничиваются тем, что любой правительственный орган, желающий хранить, модифицировать или уничтожить некий файл персональных данных, должен предварительно известить об этом Генерального директора Национального агентства по управлению и координации.

Особенностью японской системы является то, что на региональном уровне существуют более развитые системы защиты данных, чем на национальном. В настоящее время около 1 000 органов местного самоуправления (более 30% общего числа местных правительств) имеют свое собственное законодательство о защите персональных данных, обрабатываемых местными административными органами. Большинство этих местных законов содержит положения, подобные положениям национального закона. Однако имеется около 100 местных правительств, которые приняли более современное и развитое, чем на национальном уровне, законодательство о защите данных, основанное на Руководящих принципах ОЭСР.

Законодательство о защите данных в частном секторе никогда не планировалось к разработке на основании аргумента, что в Японии не сложился идеальный баланс между защитой права граждан на невмешательство в их частную жизнь и эффективным свободным течением информации. Так как основная ставка делается на Кодексы практики и "отраслевые" подзаконные акты, то не было необходимости принятия законов по защите данных для частного сектора.

Имеется целый ряд Кодексов практики, в том числе в банковской отрасли. Кроме того, в 1986 году Министерство финансов и Министерство международной торговли и промышленности выпустили совместный циркуляр относительно обработки данных потребительского кредита. В 1987 году Национальный центр информационных систем финансовой индустрии разработал для финансовых учреждений набор руководящих принципов по защите персональных данных. В

марте 1988 года Японский центр развития обработки информации ввел руководящие принципы для защиты персональных данных в частном секторе.

Министерство международной торговли и промышленности в последнее время демонстративно поощряет создание отраслевых Кодексов практики и руководящих принципов по защите данных. Многие компании добровольно подготовили свои внутренние инструкции по защите данных в соответствии с Руководящими принципами ОЭСР.

Судебные случаи по тематике «Трансграничная передача ПДн»

По сообщению Управления Роскомнадзора по РТ, мировым судом г. Кызыла по статье 13.11 КоАП РФ за незаконный сбор персональных данных осуждены сотрудники российского представительства «Американских Советов по международному образованию: АСПРЯЛ/АКСЕЛС, Инк.».

По данному факту Прокуратурой РТ проведена проверка и установлено, что сотрудники «Американских Советов по международному образованию», пренебрегая установленными правилами, без получения устного или письменного согласия родителей организовали сбор персональных данных у 94-х несовершеннолетних граждан России.

На основании материалов административного расследования американец с учетом грубого нарушения законодательства был оштрафован, а Дарье Колтушкиной вынесено предупреждение.

Заинтересовавшись данным сообщением, мы провели собственное небольшое журналистское расследование, и выяснили много любопытных деталей.

В ноябре прошлого года менеджеры АСМО Кнутсон Бо Андерс и Дарья Колтушкина в главном корпусе ТувГУ проводили отбор участников обменной программы «РЬЕХ», пришло почти 100 учеников средних школ Тывы.

Нарушив требования российского Закона, «АСМОвцы» не оформили согласия на получение персональных данных ни от школьников, ни от их родителей. Под предлогом организации выезда детей на годичную учебу в США американец и его помощница выяснили всю их подноготную. Проведением подробного анкетирования и собеседований они собрали фотографии (то есть биометрические данные), адреса электронной почты, номера телефонов, а также места учебы, проживания и данные близких родственников детей. Не обошли вниманием и особенности характера, способности и наклонности.

Несмотря на то, что по результатам тестов были отобраны единицы, американцем с помощницей были собраны и вывезены материалы о практически всех тувинских школьниках в возрасте от 15 до 17 лет, хорошо владеющих английским языком. Вопрос о том, зачем американцам нужны личные данные наших детей, и как они их используют, остается открытым.

ЗАЩИТА ПДН В КИТАЕ

Конституция Китайской Народной Республики (далее «КНР» или «Китай») гарантирует защиту достоинства личности и тайну переписки. Положения о защите ПДн содержатся в отдельных нормативно-правовых актах.

Отдельные нормативно-правовые акты, содержащие положения о защите ПДн в Китайском законодательстве

1. 5.11.2012 года было принято «Руководство по защите персональной информации в информационной системе по оказанию публичных и коммерческих услуг».

А) *Персональные данны*е — любая информацию об определенном физическом лице, которая сама по себе или в комбинации с другой информацией позволяет его идентифицировать.

Б) Оператор ПДн обязан получать согласие субъекта ПДн на обработку и сообщать ему о цели обработки, сроке хранения, мерах по защите ПДн и др.

В) При отсутствии ясно выраженного согласия субъекта ПДн, нормативного разрешения или согласия уполномоченных органов оператор ПДн не должен передавать ПДн какому-либо лицу, находящемуся за рубежом, включая любых физических лиц, проживающих за рубежом, или любых организаций и компаний, которые зарегистрированы за рубежом.

2. 25.10.2013 года был принят Закон «О защите потребителей»

А) Статья 29. При сборе и использовании персональных данных физических лиц участники предпринимательской деятельности обязаны следовать принципам законности, обоснованности и необходимости, явным образом информировать о цели, способах и пределах сбора и использования информации и получить согласие потребителя.

Б) Субъекты предпринимательской деятельности обязаны предпринимать технические и другие необходимые меры для обеспечения безопасности информации и предотвращения раскрытия или утечки ПДн потребителей.

3. Закон КНР «О деликатной ответственности» 2009 года, защищающий право на неприкосновенность частной жизни и, в частности, предусматривает ответственность медицинского учреждения за распространение ПД без согласия субъекта ПД

4. 28.12.2012 года парламентом было принято «Решение об усилении защиты информации в Интернете».

5. 19.07.2013 года было принято «Положение об электросвязи и защите персональной информации интернет-пользователей».

6. 15.03.15 года вступили в силу «Меры ответственности за нарушения прав и интересов потребителей», разработанные и принятые Государственным управлением по промышленности и коммерции Китая (SAIC).

А) Представляет особый интерес в отношении определения персональных данных в контексте защиты прав потребителя.

Согласно Мерам, к ПДн потребителя относятся следующие данные:

1) Имя;
2) Пол;
3) Профессия;
4) Дата рождения;
5) Номер паспорта;
6) Адрес;
7) Контактная информация;
8) Сведения о доходах и собственности;
9) Сведения о здоровье;
10) Привычки потребителя.

7. 1.06.2017 года вступил в силу «Закон о кибербезопасности». Закон о кибербезопасности является первым сводным законом, регулирующим практически все проблемы данной сферы в Китае. В том числе, он, конечно же, касается и ПДн.

А) ***Статья 37.***

- Хранение личных данных и других важных данных должно обеспечиваться исключительно на территории КНР.

Б) ***Статья 41.***

- Обязанности сетевых операторов в отношении защиты персональной информации, которые определены существующим законодательством и регуляторными требованиями, включая право на отслеживание соблюдения принципа законности, необходимости и уместности сбора и использования личных данных, а также право наблюдения за выполнением «требований об информировании и получении согласия» об использовании личных данных лишь в тех целях, на которые дало согласие соответствующее лицо.

В) ***Статья 42.***

- Право принимать меры защиты безопасности личных данных.
- Требования об уведомлении о нарушении защиты данных.
- Право анонимизации данных в качестве исключения в требованиях об информировании и получении согласия.

Г) ***Статья 43.***

- Право защищать индивидуальное право оценивать и вносить исправления в личную информацию.
- Право индивида требовать у сетевых операторов внести изменения в или удалить его личные данные в случае, если информация о нём ошибочна или используется в несогласованных с ним целях.

Проблемы защиты ПДн в Китае:

- отсутствие уполномоченного органа по защите ПД;
- отсутствие единого специального закона о ПД;
- отсутствие единого понятийного аппарата (ну, с этим и у нас не все гладко);
- основные правила защиты ПД содержатся в НПА, которые носят рекомендательный характер (напр., Руководство);
- отсутствие уведомления об обработке ПД и реестра операторов, осуществляющих обработку ПД.

ЗАЩИТА ПДН В США

У США нет централизованного законодательства по защите персональных данных на федеральном уровне. Существуют разные законодательные акты в разных штатах, и в разных ведомствах.

Технические и организационные требования:

1) Организации должны предпринимать необходимые шаги для защиты данных, от несанкционированного доступа и нарушений политик обработки. В некоторых штатах также на законодательном уровне закреплены минимальные требования по защите информации.

Защита биометрических ПДн:

1) Нет специализированных требований к биометрической защите ПДн.

Орган по контролю за защитой ПДн:

1) Нет единого органа по защите ПДн. Но для многих случаев Federal Trade Commission (“FTC”) является контролирующим органом.

Регистрация баз и ИС ПДн:

1) Нет требований к регистрации или уведомления обработки ПДн.

Оповещение об утечках:

Необходимо уведомлять о произошедших утечках ПДн.

ЗАКОНОДАТЕЛЬСТВО ПО ЗАЩИТЕ ПЕРСОНАЛЬНВХ ДАННЫХ В ГРЕЦИИ

Личного нормативно-правового документа в Греции нет, но используют общий регламент по защите данных в ЕС – GDPR.

ГЛАВА IV. КОНТРОЛЁР И ОБРАБОТЧИК Раздел 2 Безопасность персональных данных статья 32 безопасность обработки.

Обработчики должны осуществлять соответствующие технические и организационные меры, обеспечивающие надлежащий уровень безопасности соразмерный этим рискам, включая, среди прочего, следующее:

- псевдонимизация и криптографическая защита персональных данных;
- средства для обеспечения постоянной конфиденциальности, целостности, доступности и устойчивости систем обработки и услуг;
- средства своевременного восстановления доступности и доступа к персональным данным в случае природного или технического инцидента;
- процедура регулярной проверки и оценки эффективности технических и организационных мер, обеспечивающая безопасность обработки.

При определении надлежащего уровня безопасности, в расчет должны приниматься в том числе риски, которые представляет собой сама обработка, в особенности риски от случайного или неправомерного 138 уничтожения, потери, изменения, несанкционированного раскрытия или доступа к персональным данным переданным, сохраненным либо или иным образом обработанным.

Контролёр и обработчик должны предпринять меры для обеспечения того, чтобы любое физическое лицо, подчиняющееся контролёру или обработчику, которое имеет доступ к персональным данным, не обрабатывало их, за исключением распоряжений контролёра, кроме случаев, когда он/она обязаны действовать так согласно праву Евросоюза или государства-члена.

Статья 33 Уведомление надзорного органа об утечке персональных данных

В случае утечки персональных данных контролёр, без неоправданной задержки и, при наличии соответствующей возможности, не позднее чем через 72 часа после того, как он узнает об этом, уведомляет об утечке персональных данных компетентный надзорный орган в соответствии со Статьей 55, кроме случаев, когда эта утечка персональных

данных едва ли обернется рисками для прав и свобод физических лиц. В случае если уведомление надзорного органа не произведено в течение 72 часов, в нем должны быть указать причины задержки.

Обработчик должен уведомить контролёра без неоправданной задержки об утечке персональных данных как только ему стало известно об утечке персональных данных.

Уведомление, предусмотренное параграфом 1, должно как минимум:

- описывать характер утечки персональных данных, в том числе, когда это возможно, категории и приблизительное количество соответствующих субъектов данных, а также категории и приблизительное количество соответствующих записей персональных данных;
- сообщать наименование и реквизиты инспектора по защите персональных данных или иного контактного пункта, где может быть получена более подробная информация;
- описывать вероятные последствия утечки персональных данных;
- описывать меры, предпринятые или предполагаемые к принятию контролёром в ответ на утечки персональных, в том числе, в необходимых случаях, меры по смягчению возможных неблагоприятных последствий таких утечек.

Статья 34 Сообщение субъекту данных об утечке персональных данных

В тех случаях, когда утечка персональных данных, вероятнее всего приведет к высокому риску для прав и свобод физических лиц, контролёр должен сообщить субъекту данных об утечке персональных данных, без необоснованной задержки.

ГЛАВА V. ПЕРЕДАЧА ПЕРСОНАЛЬНЫХ ДАННЫХ ТРЕТЬИМ СТРАНАМ ИЛИ МЕЖДУНАРОДНЫМ ОРГАНИЗАЦИЯМ Статья 44 Общие принципы передачи

Любая передача персональных данных, подвергшихся обработке или предназначенные для обработки, после передачи третьей стране или международной организации, должна проводиться лишь в случаях, когда это допускается другими положениями настоящего Регламента, если условия, предусмотренные в этой Главе, соблюдаются контролёром или обработчиком, включая последующую передачу персональных данных из третьей страны или международной организации в другую третью страну или в другую международную организацию. Все положения настоящей Главы должны применяться с целью обеспечения того, чтобы уровень защиты физических лиц, гарантированный настоящим Регламентом, не был подорван.

ГЛАВА VI. САМОСТОЯТЕЛЬНЫЕ НАДЗОРНЫЕ ОРГАНЫ Раздел 2 КОМПЕТЕНЦИЯ, ЗАДАЧИ И ПОЛНОМОЧИЯ Статья 58 Полномочия

Каждый надзорный орган должен располагать всеми нижеследующими следующими полномочиями по устранению недостатков:

- выносить предупреждения контролёру или обработчику о том, что предполагаемая обработка данных способна нарушить положения настоящего Регламента;
- объявлять выговор контролёру или обработчику, если операция обработки нарушила положения настоящего Регламента;
- предписывать контролёру или обработчику соблюдать запросы субъекта данных относительно осуществления его/ее прав по настоящему Регламенту;
- предписывать контролёру или обработчику вести операции обработки в соответствии с положениями настоящего Регламента, когда это применимо, в установленном порядке в течение определенного срока;
- предписывать контролёру сообщить субъекту данных об утечке персональных данных;
- налгать временные или окончательные ограничения, включая запрет обработки;
- предписывать исправить или удалить персональные данные, либо ограничить обработку в порядке Статей 16, 17 и 18, а также уведомить об указанных мерах получателей, которым были раскрыты персональные данные в соответствии со Статьей 17 (2) и Статьей 19;
- отзывать сертификат или предписывать органу сертификации отозвать сертификат, выданный в соответствии со Статьями 42 и 43, либо предписать органу сертификации не выдавать сертификат, если требования к сертификации отсутствуют или больше не выполняются;
- налагать административный штраф в порядке Статьи 83 в дополнение или вместо мер, предусмотренных в настоящем параграфе, в зависимости от обстоятельств каждого конкретного дела;
- предписывать приостановку перемещения потока данных получателю в третьей стране или международной организации.

ГЛАВА VIII. СРЕДСТВА ПРАВОВОЙ ЗАЩИТЫ, ОТВЕТСТВЕННОСТЬ И САНКЦИИ Статья 83 Общие условия наложения административных штрафов

Каждый надзорный орган должен обеспечить, чтобы наложение административных штрафов, в порядке настоящей Статьи в отношении нарушений положений настоящего Регламента, предусмотренных в параграфах 4, 5 и 6, в каждом отдельном случае, было эффективным, соразмерным и имело сдерживающее воздействие.

Административные штрафы, в зависимости от обстоятельств каждого конкретного случая, должны налагаться в дополнение, либо вместо мер, предусмотренных пунктами (a)-(h) и (j) Статьи 58 (2). При принятии решения по вопросу наложения административного штрафа и решения о размере административного штрафа, в каждом отдельном случае должно подлежать учету следующее:

- характер, тяжесть и продолжительность нарушения, принимая во внимание характер, объем и цели соответствующей обработки, также как и количество затронутых субъектов данных, а равно и размер ущерба, понесенного ими;
- умышленный или неосторожный характер нарушения;
- любые меры, предпринятые контролёром или обработчиком, для смягчения ущерба, полученного субъектами данных;
- степень ответственности контролёра или обработчика, принимая во внимание технические и организационные меры, осуществляемые ими в соответствии со Статьями 25 и 32;
- любые соответствующие предыдущие нарушения контролёра или обработчика; (f) степень сотрудничества с надзорным органом для того, чтобы устранить нарушения и смягчить возможные неблагоприятные последствия нарушений;
- категории персональных данных, затронутых нарушением;
- способ, посредством которого надзорному органу стало известно о нарушении, в том числе, уведомил ли контролёр или обработчик об этом нарушении, и если да, то в какой степени;
- соблюдение мер, предусмотренных Статьей 58 (2), ранее было предписано против соответствующего контролёра или обработчика в отношение того же вопроса;
- соблюдение утвержденных кодексов поведения в соответствии со Статьей 40, или утвержденных механизмов сертификации, в соответствии со Статьей 42;
- любые иные отягчающие или смягчающие факторы, применимые к обстоятельствам дела, например, полученные финансовые выгоды или избежание потерь, прямо или косвенно связанных с нарушением. 3.

Если контролёр или обработчик умышленно или по неосторожности, по тем же самым или связанным с обработкой данных, нарушают несколько положения настоящего Регламента, общий размер административного штрафа не должен превышать размер, установленный для самого тяжкого нарушения.

СУДЕБНОЕ ДЕЛО ПО ТРАНСГРАНИЧНОЙ ПЕРЕДАЧЕ ДАННЫХ

М******* Г.Н. обратилась в суд с иском к АО «*******» о предоставлении информации, касающейся обработки персональных данных, компенсации морального вреда в размере 20 000 руб., взыскании расходов на представителя в размере 5 000 руб. и государственной пошлины в размере 300 руб.

5 июня 2015 г. истец направила в адрес Банка заявление о предоставлении информации, касающейся обработки персональных данных, предоставленных в рамках Договора о выпуске и обслуживании кредитной карты, а именно: подтвердить факт обработки персональных данных, сообщить правовые основания и цели обработки персональных данных, сообщить наименование и сведения о лицах, которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с АО «*******», сообщить наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению АО «*******».

До настоящего времени запрашиваемая информация истцу не предоставлена, что нарушает права истца.

Незаконными действиями банка истцу причинен моральный вред, который она оценивает в 20 000 руб.

При заключении Договора кредитной карты в Заявлении-анкете, истец выразила свое согласие на обработку всех своих персональных данных Банком любыми способами, в том числе третьими лицами, включая осуществление сбора, систематизацию, накопление, хранение, обновление, уточнение (проверка), изменение, использование и распространение (включая передачу), в том числе воспроизведение, электронное копирование и трансграничную передачу … с целью выпуска, обслуживания кредитных карт, для создания информационных систем персональных данных Банка, в целях предоставления информации третьим лицам, которые по договору с Банком осуществляют деятельность по обеспечению погашения должниками просроченной задолженности.

Таким образом, Банк при заключении Договора получил согласие истца на обработку персональных данных в соответствии с требованием вышеуказанного Федерального закона «О персональных данных».

******* 2015 г. истец обратилась в Банк с требованием предоставить информацию, касающуюся обработки персональных данных.

Банк в соответствии со ст. 20 Федерального закона «О персональных данных» ******* 2015 г. направил истцу ответ на заявление от ******* 2015 г.

При таких обстоятельствах, учитывая, что Банк дал ответ на заявление истца, права М******* Г.Н. не нарушены.

Кроме того, истец в силу ст. 56 ГПК РФ не представила суду доказательств, подтверждающих факт нарушения Банком порядка обработки ее персональных данных.

Суд также учитывает, что требования М******* Г.Н. об обязании предоставить ей информацию о лицах, допущенных к обработке ее персональных данных, включая фамилию, имя, отчество и адрес не основаны на положениях ч. 7 ст. 14 Федерального закона «О персональных данных».

Учитывая, что банком не допущено нарушения прав истца как потребителя и заемщика, морально-нравственные страдания М******* Г.Н. причинены не были, порядок обработки персональных данных истца Банком не нарушался, оснований для компенсации морального вреда не имеется.

В удовлетворении иска М******* Г******* Н******* к АО «*******» о предоставлении информации, компенсации морального вреда и судебных расходов - отказать.

СОСТАВ ЗАКОНОДАТЕЛЬСТВА АРМЕНИИ, ОТРАЖАЮЩЕГО ВОПРОСЫ ЗАЩИТЫ ПДН

Обязанности оператора при сборе персональных данных

1. При обработке персональных данных оператор обязан, по требованию субъекта персональных данных, предоставить субъекту персональных данных информацию, предусмотренную Законом.
2. В случае неполных, устаревших, недостоверных, незаконно полученных или не являющихся необходимыми для заявленной цели обработки персональных данных, оператор персональных данных обязан предпринять необходимые действия для их дополнения, обновления, исправления или уничтожения.
3. Оператор обязан письменно разъяснить субъекту персональных данных последствия отказа от предоставления своих персональных данных, а также права субъекта персональных данных.
4. Если персональные данные были получены не от субъекта персональных данных, за исключением случаев, если персональные данные были предоставлены оператору на основании закона или если персональные данные являются общедоступными, оператор до начала обработки таких данных обязан предоставить субъекту персональных данных следующую информацию:

- Имя (фамилия, имя, отчество) и местонахождение или адрес (фактическое место проживания) оператора или его представителя (если таковой имеется),
- цель и правовую основу обработки персональных данных, перечень обрабатываемых данных,
- круг вероятных пользователей персональных данных
- установленные Законом права субъекта персональных данных.
- Меры по обеспечению безопасности персональных данных при их обработке и обязанности оператора

1. Оператор обязан уничтожить или заблокировать персональные данные, не являющиеся необходимыми для достижения законной цели.
2. Оператор при обработке персональных данных обязан использовать шифровальные (криптографические) средства для защиты информационных систем, содержащих персональные данные от случайного доступа к ним, неправомерного использования, записи, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

3. Оператор обязан ограничить доступ к соответствующим технологиям обработки персональных данных лицам, не имеющим полномочий, а также обеспечить официальному оператору этих систем доступ только к тем данным, которые подлежат обработке с его стороны, а также к данным, которыми разрешено пользоваться.
4. Требования по обеспечению безопасности обработки персональных данных в информационных системах, а также требования к физическим носителям информации биометрических персональных данных и к технологиям по хранению персональных данных вне информационных систем должны быть установлены решением правительства Республики Армения (решение пока не принято).
5. Операторы персональных данных, или предусмотренные Законом иные лица, обязаны соблюдать конфиденциальность персональных данных как в процессе выполнения служебных обязанностей, связанных с обработкой персональных данных, так и после его окончания.

5-ая глава Закона устанавливает также:
1. обязанности оператора персональных данных в случае письменного запроса субъекта или уполномоченного органа персональных данных об ознакомлении с персональными данными в случае обнаружения нарушений со стороны оператора или уполномоченного лица,
2. обязанности оператора персональных данных в процессе устранения нарушений закона, допущенных при обработке персональных данных, в процессе корректировки, блокирования или уничтожения персональных данных,
3. обязанность уведомления уполномоченного органа об обработке персональных данных.

Следует также отметить регулирование, в соответствии с которым оператор, в случае оспаривания достоверности или законности обработки персональных данных на основании запроса субъекта персональных данных или уполномоченного органа по защите персональных данных, обязан заблокировать персональные данные, касающиеся субъекта персональных данных, с момента получения запроса до завершения инспекционной деятельности.

Уполномоченный орган по защите персональных данных

Защита персональных данных в Республике Армения осуществляется Агентством по защите персональных данных Министерства юстиции РА (далее Уполномоченный орган). Агентство назначено Уполномоченным органом в соответствии с приказом правительства РА 1188-Н от 20-го сентября 2012 года. Уполномоченный орган действует в

соответствии с Законом и другими правовыми актами, в частности, согласно приказу правительства РА 734-Н от 2-го июля 2015 года.

Уполномоченный орган по защите персональных данных действует независимо, в соответствии с Законом и другими правовыми актами.

Уполномоченный орган осуществляет следующие функции, предусмотренные Законом:

1. по своей инициативе, или согласно соответствующему запросу, проверяет соответствие обработки персональных данных требованиям Закона;
2. в случае нарушения требований Закона применяет административные санкции, установленные Законом;
3. требует заблокировать, приостановить или прекратить обработку персональных данных, нарушающую требования Закона;
4. в случае наличия обоснований, предусмотренных Законом, требует от оператора исправление, изменение, блокирование или уничтожение персональных данных;
5. по результатам изучения уведомления оператора относительно обработки персональных данных, полностью или частично запрещает обработку персональных данных;
6. ведет реестр операторов персональных данных;
7. признает уровень защищенности электронных систем, обрабатывающих персональные данные юридических лиц, удовлетворительным и вносит их в реестр;
8. проверяет устройства, документацию, применяемую в обработке персональных данных, а также существующие данные и компьютерные программы;
9. в предусмотренных Законом случаях обращается в суд;
10. соблюдает конфиденциальность персональных данных, полученных им, или доверенных ему в процессе своей деятельности;
11. обеспечивает защиту прав субъекта персональных данных;
12. расследует заявления физических лиц относительно обработки персональных данных, и принимает решения в рамках своих полномочий;

13. раз в год представляет публичный отчет о ситуации в сфере защиты персональных данных, и о деятельности за прошедший год;
14. на основании заявлений операторов проводит исследования и консультации относительно обработки персональных данных, или делится наилучшим опытом обработки персональных данных;
15. сообщает правоохранительным органам, в случаях возникновения подозрений о нарушениях уголовного характера в процессе своей деятельности.

Решения уполномоченного органа по защите персональных данных могут быть опротестованы в судебном порядке.

Предусмотренные Законом полномочия уполномоченного органа по защите персональных данных осуществляются средствами государственного бюджета и финансируются отдельной строкой.

Назначение руководителя уполномоченного органа, его полномочия и требования к нему

1. Руководитель уполномоченного органа назначается Премьер-министром Республики Армения сроком на 5 лет с представления Министра юстиции Республики Армения, на основании совместных рекомендаций, по крайней мере, пяти неправительственных организаций, осуществляющих правозащитную деятельность. Кандидат в руководители уполномоченного органа, представленный Премьер-министру Республики Армения Министром юстиции, должен быть из списка кандидатов, представленных общественными организациями.
2. Порядок представления кандидатов общественными организациями был установлен Решением Правительства Республики Армения 736-Н от 2-го июля 2015 года.
3. Руководитель уполномоченного органа по защите персональных данных руководит деятельностью уполномоченного органа и несет ответственность за осуществление полномочий уполномоченного органа.
4. Одно и то же лицо не может быть назначено на должность руководителя уполномоченного органа два раза подряд.
5. Руководитель уполномоченного органа:

- Должен иметь высшее образование, пользоваться высоким авторитетом и иметь, по крайней мере, 5-и летний опыт руководящей работы;
- должен воздерживаться от действий, ставящих под сомнение его беспристрастность и независимость.

1. Руководитель уполномоченного органа по защите персональных данных освобождается от руководящей должности на следующих основаниях:

- на основании письменного заявления;
- при достижении 65 лет (пенсионный возраст), или истечении срока полномочий;
- при избрании или назначении на другую должность, или переходе на другую работу, несовместимую с должностью руководителя уполномоченного органа;
- вследствие отсутствия на службе более 120-и дней подряд, или более 140-а дней в течение последних 12-и месяцев, в связи с временной потерей трудоспособности, за исключением отпуска по беременности и родам или по уходу за ребенком;
- вследствие отсутствия на службе более пяти дней подряд без уважительной причины;
- на основании вступившего в силу решения суда, по признанию недееспособным или с ограниченными возможностями, безвестно отсутствующим или умершим;
- в соответствии со вступившим в силу приговором суда.

Передача персональных данных третьим лицам и иностранным государствам

1. Без согласия субъекта персональных данных, оператор может передавать персональные данные третьим лицам, или предоставлять возможность использования данных в том случае, если это предусмотрено законом и имеет достаточную степень защиты.

2. Без согласия субъекта персональных данных, оператор может передавать специальные категории персональных данных третьим лицам или предоставлять возможность использования данных, если:

- в соответствии с законом или межгосударственным соглашением оператор данных является оператором специальных категорий персональных данных, передача таких данных прямо предусмотрена законом и имеет достаточную степень защиты;
- в предусмотренных законом исключительных случаях специальные категории персональных данных могут передаваться в целях охраны жизни, здоровья или свобод субъекта данных.

Передача персональных данных иностранным государствам

Передача персональных данных иностранным государствам может осуществляться при наличии согласия субъекта персональных данных, или если передача данных вытекает из целей обработки персональных данных и (или) необходима для осуществления этих целей.

Без разрешения уполномоченного органа, передача персональных данных иностранным государствам может осуществляться на территории другого государства, если в этом государстве обеспечивается надлежащий уровень защиты персональных данных. Надлежащий уровень защиты персональных данных считается обеспеченным, если:

- персональные данные передаются в соответствии с международным соглашением;
- персональные данные передаются на территорию других государств, включенных в официальный список, опубликованный Уполномоченным органом;

Персональные данные могут передаваться на территорию государства, не обеспечивающего надлежащий уровень защиты только с разрешения Уполномоченного органа, в том случае, если персональные данные передаются в соответствии с соглашением, по которому предусмотрены гарантии защиты персональных данных, установленные Уполномоченным органом как гарант надлежащей защиты. В таких случаях оператор персональных данных обязан, прежде чем передавать данные в такое государство, отправить в Уполномоченный орган письменный запрос о получении разрешения. Оператор персональных данных обязан указать в запросе государство, на территорию которого передаются персональные данные, описание (наименование, организационно-правовая форма) субъекта получателя персональных данных, описание персональных данных (содержание), цель обработки и передачи персональных данных, соглашение или проект соглашения.

Уполномоченный орган в течение 30-и дней обязан дать разрешение, или отклонить запрос. Уполномоченный орган может потребовать у оператора персональных данных дополнительную информацию с соблюдением сроков рассмотрения запроса. В случае если Уполномоченный орган считает, что договорные гарантии не достаточны, он обязан указать необходимые изменения, способные обеспечить гарантии защиты персональных данных.

Уполномоченных орган по защите персональных данных регулярно, но не реже одного раза в год, обязан пересматривать список стран, обеспечивающих надлежащий уровень защиты персональных данных, и публиковать поправки в официальном Журнале и на своем официальном сайте.

Персональные данные, которыми обладают органы государственной власти, могут быть переданы иностранным государственным органам только в рамках межгосударственного соглашения, а негосударственным органам в соответствии с нормами Закона.

Административная ответственность

Кодексом РА об Административных правонарушениях (статья 189.17), предусмотрена административная ответственность за нарушение закона «О защите персональных данных».

В частности, в Кодексе установлено следующее:

1. Нарушение установленного Законом порядка сбора, записи, ввода, систематизации, организации, корректировки, хранения, использования, изменения, восстановления, передачи персональных данных, если данное действие не содержит признаков преступления, влечет наложение штрафа в размере от двухсот до пятисот минимальных заработных плат (приблизительно от 410 до 1.000 долларов США);
2. Нарушение порядка уничтожения или блокирования персональных данных, установленного той же статьей Закона, если данное действие не содержит признаков преступления, влечет наложение штрафа в размере от трехсот до пятисот минимальных заработных плат (приблизительно от 620 до 1.000 долларов США).
3. Если в процессе сбора персональных данных оператор персональных данных отказывается предоставить по требованию субъекта персональных данных сведения, предусмотренные Законом, нарушает порядок предоставления сведений или не разъясняет причины и последствия отказа, назначается штраф в размере от ста до двухсот минимальных заработных плат (приблизительно от 200 до 410 долларов США).
4. Не уведомление или нарушение оператором персональных данных процедуры уведомления Уполномоченного органа по защите персональных данных, влечет за собой наложение штрафа в размере от пятидесяти до ста минимальных заработных плат (приблизительно от 100 до 200 долларов США).
5. Неиспользование в процессе обработки персональных данных средств криптографии в случае, если данное действие не содержит признаков преступления, влечет за собой наложение штрафа в размере ста минимальных заработных плат (приблизительно 200 долларов США).
6. Нарушение требований по обеспечению безопасности обработки персональных данных в информационных системах, а также требований к физическим носителям информации биометрических персональных данных и к

технологиям по хранению персональных данных вне информационных систем, влечет за собой наложение штрафа в размере от ста до двухсот минимальных заработных плат (приблизительно от 200 до 410 долларов США).

7. Несоблюдение конфиденциальности персональных данных в процессе исполнения рабочих обязанностей, связанных с обработкой персональных данных, или после их завершения, а также несоблюдение конфиденциальности персональных данных оператором персональных данных или другими лицами, предусмотренными Законом, влечет за собой наложение штрафа в размере от двухсот до трехсот минимальных заработных плат (около от 410 до 620 долларов США).

8. Субъект, совершивший вышеуказанные действия, освобождается от административной ответственности, если допущенные нарушения были им устранены, и доказательства уполномоченному органу были предъявлены в рамках срока, установленного Уполномоченным органом или до принятия решения об административной ответственности.

Уголовная ответственность

Уголовный кодекс Республики Армения (статья 144) предусматривает уголовную ответственность за незаконный сбор, хранение, использование и распространение информации о частной (личной и семейной) жизни лиц. Кодексом предусмотрено, что использование или распространение, сбор и хранение информации о частной (личной, семейной) жизни человека посредством публичных выступлений, публично демонстрируемых произведений или средств массовой информации без его разрешения, если это не предусмотрено Законом, влечет за собой наложение штрафа в размере от двухсот до пятисот минимальных заработных плат (около от 410 до 1.000 долларов США), или наказание в виде лишения свободы на срок от одного до двух месяцев.

Состав законодательства Кипра, отражающего вопросы защиты ПДн

Введение

Защита персональных данных является основополагающим правом, вытекающим из статьи 8 ЕКПЧ, которая является правом на уважение частной и семейной жизни. Как национальное, так и европейское право должно обеспечивать гарантии, чтобы предотвратить несоответствие статьи, а также гарантировать, что обработка и хранение персональных данных не является чрезмерной в отношении цели, которую они обрабатывают и сохраняют.

Действующее законодательство на Кипре

Действующим законодательством для обработки и защиты персональных данных на Кипре является Закон о персональных данных (защита личности) 2001 года («Закон»).

Закон основан на Европейской директиве 95/46 / ЕС Европейского парламента и Совета 24 октября 1995 года («Директива») и имеет двоякую цель:

- защита основных прав и частной жизни отдельных лиц и обеспечение свободного распространения персональных данных в государствах-участниках для достижения экономического и социального прогресса; а также
- техническое и научное сотрудничество в постоянно растущем информационном и телекоммуникационном обществе.

Новые правила

Быстрые технологические разработки и увеличение сбора и обмена персональными данными вызвали новые проблемы для защиты персональных данных. Технология позволила частным компаниям и государственным органам беспрепятственно использовать персональные данные. Кроме того, физические лица все чаще предоставляют личные данные как на публичной, так и на глобальном уровнях.

Хотя цели Директивы остаются в силе, она не смогла предотвратить юридическую неопределенность, и восприятие того, что существующий значительный риск для защиты физических лиц, по-прежнему сохраняется. Кроме того, различия в уровне защиты персональных данных и обработке персональных данных в государствах-участниках представляют собой препятствие для осуществления экономической деятельности в Европейском союзе.

Эти события сделали требование о создании более сильной и согласованной системы защиты данных в Европейском союзе более неизбежным.

Новые правила (ЕС) 2016/679 Европейского парламента и Совета 27 апреля 2016 года («Положение») обеспечивают правовую определенность и прозрачность для экономических операторов, то есть юридические предприятия и физические лица государств-участников, оснащены тем же уровнем прав и обязательств, которые подлежат исполнению, для обеспечения постоянного контроля обработки персональных данных.

Ключевые изменения, внесенные в Правила

- **Увеличение территориальной сферы**

Новое правило распространяется на все компании, которые обрабатывают персональные данные субъектов, проживающих на территории Европейского Союза. Новое правило будет применяться к обработке персональных данных контроллерами и процессорами в ЕС независимо от того, происходит ли обработка в ЕС или нет. Кроме того, предприятиям, не входящие в ЕС, но обрабатывающие данные граждан ЕС, также придется назначать представителя в ЕС.

- **Штрафы**

С новым регулированием существует более строгая политика в отношении штрафов:

– штраф в размере до €10.000.000 евро или 2% от общего мирового, годового оборота за предыдущий год, в зависимости от того, что выше, за нарушение обязательств, установленных для контролеров и обработчиков данных, включая условия, необходимые для получения согласия ребенка (статья 8), неспособность сохранить идентификацию

персональных данных субъектов, при обработке данных (статья 11), отказ в применении защиты механизмов данных по дизайну и по умолчанию (статья 25), нарушение обязанностей сотрудника по защите данных (статья 39) и неспособность контролирующих органов контролировать соблюдение кодекса поведения (статья 41).

– штраф в размере до 20 000 000 евро или 4% от общего мирового, годового оборота за предыдущий финансовый год, в зависимости от того, что выше, будет наложено там, где есть нарушение основных условий обработки данных (статьи 5, 6 и 7), нарушение прав персональных данных субъектов (статьи 12-22), в случае нарушения требований, изложенных в Положении о передаче персональных данных получателю в третьей стране или международной организации (статья 44-49), или соблюдать указания контролирующего органа в соответствии со статьей 58.

- **Согласие**

Положение устанавливает новое определение «согласия субъекта данных»; как конкретное, свободно предоставленное, информированное и недвусмысленное указание на пожелания, которым он или она путем заявления или четким утвердительным действием, соглашается с обработкой персональных данных, относящихся к нему или ей.

Были усилены условия получения согласия от субъектов данных. Впредь просьба о согласии должна быть дана в письменной декларации в различной и легкодоступной форме четким и понятным языком. Субъекты данных должны быть проинформированы о цели обработки данных, а также проинформированы о своем праве отозвать данное согласие.

- **Сотрудники по защите данных**

Сотрудник по защите данных («DPO») является лицом, назначенным контроллером данных при определенных обстоятельствах: a) когда обработка данных выполняется государственным органом, b) когда обработка данных контроллера данных требует регулярного и систематического мониторинга субъектов данных в крупном масштабе или c) когда обрабатывающая деятельность контроллера состоит из обработки в больших масштабах специальных категорий данных (например, данные, раскрывающие расовое или этническое происхождение, политические мнения, религиозные убеждения и т. д.) и личные данные, касающиеся к уголовным обвинительным приговорам.

DPO может быть членом персонала контролера и назначается на основе профессиональных качеств (то есть экспертных знаний о законах и практике защиты данных) и может выполнять задачи, перечисленные ниже:

- информировать и консультировать контроллера данных, процессор и сотрудников, которые выполняют обработку данных, свои обязательства в соответствии с положениями о защите данных нового Положения и любым другим положением ЕС;
- контролировать соответствие контроллера или процессора политике Положения в отношении защиты персональных данных;
- осуществлять мониторинг и предоставлять рекомендации в отношении оценок воздействия защиты данных;
- сотрудничать с надзорным органом (на Кипре надзорным органом является Канцелярия Уполномоченного по защите персональных данных);

действовать в качестве контактного пункта между надзорным органом, связанным с обработкой персональных данных;

Судебные случаи по тематике «Трансграничная передача ПДн».

Решение Суда Европейского Союза по иску против Facebook.

Суд Европейского Союза принял решение, которое может привести к тому, что передача персональных данных из Европы в США будет признана противоречащей требованиям законодательства ЕС о защите персональных данных. Это решение было принято 6 октября 2015 года на основании обращения австрийского юриста Maximilian Schrems, аспиранта Венского Университета, в Ирландский суд с жалобой против Facebook. Он жаловался, что Facebook хранит его персональные данные в США, включая те, которые он удалил со своей страницы, и тем самым нарушает его права на охрану персональных данных. В качестве аргумента о существовании угрозы Максимилиан Шремс ссылался на признание Эдварда Сноудена о том, что американские спецслужбы получали информацию о гражданах от Google, Apple и Facebook.

В Еропейском Союзе действует директива о защите персональных данных, которая предусматривает, что персональные данные могут передаваться в другие страны, если при этом в стране, куда они передаются, обеспечивается определенный уровень их защиты. Вопрос о том, обеспечивается ли защита персональных данных в конкретной стране, может решаться Комиссией ЕС. Но следить за соблюдением требований директивы должны специально уполномоченные органы каждого государства – члена ЕС.

В своем решении Суд ЕС указал, что указанные выводы Комиссии никак не влияют на обязанности специально уполномоченных органов в государствах-членах ЕС следить за охраной персональных данных. И более того, решение Комиссии не является обязательным для этих органов. Но при этом Суд также рассмотрел и само решение Комиссии и признал его недействительным. Выводы Суда базируются на том факте, что на самом деле Комиссия, принимая решение Safe Harbour Decision, не изучала положения законодательства США на предмет охраны персональных данных. Кроме того, safe harbor program, которую обязывались соблюдать компании, никак не влияет на действия государственных органов США. На самом деле власти США имеют возможность почти неограниченного доступа к персональным данным. Вторым аргументом Суда стал тот факт, что законодательством США не предусматривает возможность

обращений пользователей с просьбой изменить их данные или удалить их, если они являются не точными или недостоверными. Все это идет в разрез с двумя требованиями законодательства Европейского Союза: об охране персональных данных и об обеспечении доступа к правосудию. Единственное, что последует за решением Суда ЕС, может ли Facebook передавать персональные данные европейских пользователей в США, будет рассмотрен специально уполномоченным органом в Ирландии.

Персональные данные и защита частной жизни в Молдове

Конституция РМ в ст.28 предусматривает, что государство уважает и охраняет интимную, семейную и частную жизнь. Согласно ст. 30 Конституции государство обеспечивает тайну писем, телеграмм и других почтовых отправлений, телефонных переговоров и иных законных видов связи. Отступления от этих положений допускаются законом в случаях, когда это необходимо в интересах национальной безопасности, экономического благосостояния страны, общественного порядка и в целях предотвращения преступлений.

Неприкосновенность интимной, семейной и частной жизни относится к объектам гражданских прав и защищается всеми предусмотренными законом способами, прежде всего, в исковом порядке, путем возмещения причиненного морального вреда. Суды по заявлениям граждан присуждают им, как правило, сравнительно небольшие компенсации за причиненный моральный ущерб в связи с нарушением неприкосновенности частной жизни: распространением информации в СМИ, опубликованием личной переписки, раскрытием фактов личной жизни.

Законодательство страны в сфере обработки персональных данных, состоит, в том числе, из **Конвенции Совета Европы о защите физических лиц при автоматизированной обработке данных личного характера**, дополнительного протокола к этой Конвенции и других международных соглашений, стороной которых является Молдова. Республика Молдова подписала данную Конвенцию в мае 1998 года, ратифицировала ее постановлением Парламента в июле 1999 года. Конвенция вступила в силу для Молдовы с 1 июня 2008 года.

Вместе со сдачей на хранение ратификационной грамоты Конвенции, были представлены декларации, в которых власти заявили, что не будут применять Конвенцию в отношении обработки персональных данных физическими лицами исключительно для личных и семейных нужд (с условием, что они не нарушают права субъектов персональных данных), а также в отношении обработки персональных данных, относящихся к информации, являющейся государственной тайной. В то же время было заявлено, что Конвенция будет применяться в отношении персональных данных, которые не подвергаются автоматизированной обработке. Кроме того, Молдова назначила Национальный центр по защите персональных данных в качестве компетентного органа по исполнению положений Конвенции и поддержанию отношений взаимопомощи с другими государствами-участниками.

В апреле 2010 года был подписан, а в сентябре 2011 года ратифицирован **Дополнительный протокол к Конвенции о защите физических лиц при автоматизированной обработке данных личного характера**, касающийся органов контроля и трансграничной передачи данных. Он вступил в силу для Республики Молдова с 1 января 2012 года.

Действующий **Закон о защите персональных данных** был принят Парламентом в 2011 г. Закон вступил в силу в апреле 2012 г., его целью стало обеспечение защиты основных прав и свобод физического лица при обработке его персональных данных, в особенности права на неприкосновенность интимной, семейной и частной жизни. Им регулируются правоотношения, возникающие при обработке персональных данных полностью или частично автоматизированными средствами, а также при обработке средствами, отличными от автоматизированных, персональных данных, составляющих часть системы учета или предназначенных для введения в такую систему.

Состав законодательства Польши, отражающий вопросы защиты ПДн

ЗАКОН ПОЛЬШИ О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

ОТ 29 АВГУСТА 1997 Г.

Закон применяется как в отношении государственных органов власти, территориальных органов самоуправления, так и в отношении государственных и муниципальных образований.

Закон также применяется:

- к негосударственным организациям, выполняющим государственные задачи,
- к физическим и юридическим лицам и не являющимися юридическими лицами образованиям, если они по роду своей деловой или профессиональной деятельности или для выполнения установленных целей связаны с обработкой персональных данных постоянно или временно проживающих на территории Республики Польша или третьей страны, если они связаны с обработкой персональных данных техническими устройствами, расположенными на территории Республики Польша.

Обработка персональных данных разрешается только если:

1) субъект данных дал свое письменное согласие, кроме случаев, когда обработка заключается в удалении персональных данных,

2) обработка необходима для осуществления прав и обязанностей, вытекающих из законных оснований,

3) обработка необходима для выполнения договора, в котором субъект данных является одной из сторон, или для принятия мер по требованию субъекта данных до заключения договора,

4) обработка необходима для выполнения предусмотренных законом задач в государственных интересах,

5) обработка следует законным интересам операторов или получателей данных, при условии, что обработка не нарушает права и свободы субъекта данных.

Оператор обязан осуществлять соответствующие рискам и категории защищаемых данных технические и организационные меры для защиты обрабатываемых персональных данных, в частности, защищать данные от несанкционированного доступа, обработки с нарушением закона, любого изменения, потери, повреждения или разрушения. Оператор должен хранить документацию, описывающую методы обработки данных и меры, упомянутые в пункте 1. Оператор должен назначить администратора по информационной безопасности, который контролирует соблюдение принципов обеспечения безопасности согласно п.1, если оператор не делает это сам.

Выполнять обработку данных разрешено только лицам, уполномоченным оператором.

Оператор обязан обеспечить контроль над тем, какие данные, когда и кем были введены в систему хранения данных и кому они передаются.

Оператор обязан представить систему хранения данных на регистрацию Главному инспектору. Вышесказанное не относится к случаям, перечисленным в пункте 1 статьи 43.

Уведомление, касающееся представленной на регистрацию системы хранения данных, должно содержать следующее:

1) заявление на включение системы хранения персональных данных в реестр,

2) указание субъекта, работающего с системой хранения данных, и адрес его местонахождения или местожительства, включая идентификационный номер в реестре предприятий (если есть) и законные основания, по которым он или она уполномочен работать с системой хранения данных; в случае, предусмотренном статьей 31a, указание субъекта и адрес его местонахождения или местожительства,

3) цель обработки данных,

3a) описание категорий субъектов данных и возможности обработанных данных,

4) информацию о способах и средствах сбора и обнаружения данных,

4a) информацию о получателях или категориях получателей, которым могут быть переданы данные,

5) описание технических и организационных мероприятий, применявшихся в указанных в статьях с 36 по 39 целях,

6) информацию о способах и средствах выполнения технических и организационных условий, определенных в положениях статьи 39a,

7) информацию, касающуюся возможной передачи данных третьей стране.

Оператор должен быть обязан уведомлять Главного инспектора о любых изменениях, затрагивающих указанную в параграфе 1 информацию, в течение 30 дней после даты изменения, внесенного в систему хранения данных. Положения о регистрации систем хранения персональных данных соответствующим образом применяются к уведомлению об изменениях.

Передача персональных данных в другую страну может осуществляться только в том случае, если страна назначения гарантирует, по меньшей мере, такой же уровень защиты персональных данных, как на территории Республики Польша.

Положение вышеупомянутого пункта 1 не применяется в отношении передачи персональных данных, требуемой на законных основаниях или необходимой по условиям любого ратифицированного международного соглашения.

Однако оператор может передать персональные данные в другую страну при условии, что:

1) субъект данных предоставил свое письменное согласие,

2) передача необходима для выполнения договора между субъектом данных и оператором или происходит по заявлению субъекта данных,

3) передача необходима для выполнения договора, заключенного в интересах субъекта данных между оператором и другим субъектом,

4) передача необходима или требуется в государственных интересах или организаций, обладающих правами требования,

5) передача необходима для защиты жизненных интересов субъекта данных,

6) передача касается данных, находящихся в открытом доступе.

Лицо, которое, являясь оператором системы хранения данных, хранит персональные данные образом, несовместимым с целью, во имя которой была создана система, должно быть наказано ограничением или лишением свободы на срок до 1 года.

Если нарушение имело непреднамеренный характер, нарушитель должен быть наказан ограничением или лишением свободы на срок до 1 года.

Лицо, которое, являясь оператором, не информирует субъекта данных о его правах или не обеспечивает его информацией, которая сделала бы возможным извлечение им выгоды из положений настоящего закона, должно быть наказано частичным ограничением свободы или тюремным заключением на срок до 1 года.

Rozporządzenie o Ochronie Danych Osobowych (RODO)

Данное законодательство касается абсолютно всех фирм и государственных организаций Польши, которые накапливают и используют персональные данные физических лиц. Что интересно – RODO должны учесть в своей деятельности абсолютно все организации государственных органов, ранее на них не распространялось действие такого законодательства. Сегодняшние изменения касаются как больших фирм, так и каждое госучреждение Польши, даже те небольшие фирмы, в которых работает всего несколько человек, интернет-магазины, школы, и все-все, кто так или иначе хранит данные о физических лицах.

Новое законодательство вводит ряд обязанностей, по новому описывает ответственность, а так же финансовые санкции. Новые штрафы могут измеряться в сотнях тысяч злоты или даже в миллионах евро, в зависимости от фирмы, которая будет наказана.

Кроме этого вводится ряд других изменений:

- расширение категорий ответственности за нарушение,
- на фирмах будет определен руководитель, который непосредственно отвечает за хранение персональных данных,
- вводится понятие инспектора персональных данных (IOD),
- вводится обязательство проведения аудитов безопасности, а также ведения журналов рисков и нарушений.
- Это только некоторые изменения, которые требуют организационных изменений в вашей фирме.

За нарушения законодательства о охране персональных данных будет ответчать непосредственно руководитель фирмы, отдела, школы, госорганизации. Ответственность является непосредственной и назначение инспектора охраны персональных данных в фирме или передача этой функции сторонней фирме не освобождает от этой ответственности. А потому каждый президент правления, директор, бурмистр, мэр города должен соответственным образом приготовиться к RODO. Руководитель предприятия является ответственным лицом как перед контролирующим органом, так и перед судами соответствующих инстанций. Нет возможности перенести эту ответственность на кого-то из работников предприятия.

Инспектор охраны данных (IOD) – это новая функция ответственного лица в организации, которое занимается не только вопросами персональных данных, но на котором лежит обязанность уведомления органов контроля о нарушениях. Понятие администратора персональных данных (ABI), которое существовало ранее перестаёт при этом существовать.

Любая компания, будь то Google, Facebook или PayPal, которая обрабатывает персональные данные резидентов союза, обязана соблюдать предписания RODO. В связи с этим, ваши почтовые ящики уже должны быть забиты сообщениями от компаний, которые массово переписывают свои пользовательские соглашения.

Определение IOD является обязательным для юридических лиц, которые во время ведения своей деятельности обрабатывают такие типы персональных данных, отсутствие безопасности которых может привести к нарушению прав и свобод физических лиц, к примеру дети.

Инспектор Персональных Данных IOD имеет обязательство уведомлять контролирующие органы о нарушении безопасности персональных данных на предприятии в течении 72 часов от момента возникновения нарушения.

В некоторых случаях есть необходимость уведомления непосредственно физических лиц, которых касается инцидент (утечка).

Одно из изменений, которое навязывает нам RODO, является новое обязательство для инспектора персональных данных на предприятии – ведение журнала-реестра нарушений. Согласно законодательству IOD должен документировать любые нарушения безопасности персональных данных, суть самих нарушений, а так же описывать действия, которые были предприняты в этой связи.

Ведение документации подобным образом должно дать возможность контролирующим органам возможность проверить, соблюдаются ли фирмой правила RODO в отношении ведения такой документации, а так же возможность проверки уведомления контролирующего органа о такого рода нарушениях.

Администратор данных должен обеспечить возможность выражение согласия на хранение персональных данных детей родителями (в первую очередь это касается сервисов в Интернете).

RODO не обязает регистрировать реестры данных, которые содержат персональные данные. Однако вводят обязательство вести внутренний реестр обработки таких данных, который должен включать в себя такую информацию:

причина обработки конкретных персональных данных, описание категории персональных данных, реестры нарушений, данные ответственных лиц, которые ответственны за обработку конкретного объекта данных на

Согласие на обработку данных может иметь форму не только заявления, но и четкого подтверждения

RODO признает право физического лица требовать от организаций, которые хранят персональные данные физического лица, удаления персональных данных о себе, такая просьба не имеет возможности отказа.

За нарушение законодательства RODO могут быть применены штрафные санкции в размере до 20 000 000 евро, или в размере до 4% от общего оборота предприятия за предыдущий финансовый год. Следует признать, что такой размер наказания аномально высок, и GIODO (Generalny Inspektor Ochrony Danych Osobowych) будет применять национальные правила Польши, касающиеся санкций за ненадлежащее выполнение информационных обязательств.

Судебные случаи по тематике «Трансграничная передача ПДн»

Передача банком персональных данных третьим лицам

Судебная коллегия по гражданским делам Московского городского суда в ноябре 2016 года рассмотрела дело № 33-46283, в котором гражданка просила суд обязать АО Банк «Русский стандарт» прекратить передачу и обработку ее персональных данных (ПДн), уничтожить их и взыскать компенсацию морального вреда, а также расходов по оплате услуг представителя.

Суть спора

Между банком и гражданкой был заключен договор потребительского кредита, но полностью возвратить суммы долга по кредиту, процентам по кредиту и пеням гражданка не смогла.

По ее мнению, банк, в нарушение норм действующего законодательства, без ее согласия, передал ее персональные данные другому лицу - ООО «Эверест», чем нарушил положения ФЗ от 27.07.2006 № 152-ФЗ «О персональных данных» и причинил ей нравственные и моральные страдания.

Позиция Симоновского районного суда г. Москвы

Симоновский районный суд г. Москвы в июле 2016 года установил, что при заключении договора гражданка сообщила банку свои персональные данные (фамилию, имя, отчество, год, месяц, дату и место рождения, адрес, семейное, социальное и имущественное положение, образование, профессию, доходы, контактные телефоны, другую информацию), предъявила паспорт гражданина РФ, а также действуя по своей волей и в своем интересе, дала согласие на их обработку (в том числе, на сбор, систематизацию, накопление, хранение, уточнение, обновление, изменение, распространение, передачу (включая трансграничную передачу), обезличивание, блокирование и уничтожение).

В соответствии с условиями договора (п. 12.10), такое согласие дается:

В отношении любой информации, относящейся к клиенту, полученной как от самого клиента, так и от третьих лиц включая: фамилию, имя, отчество, данные документа, удостоверяющего личность, гражданство, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, исполнение обязательств клиента по договору, договору залога, равно как и по иным договорам, заключенным между банком и клиентом;

Для целей исполнения договора и/или договора залога, осуществления обслуживания кредита и сбора задолженности (в том числе в случае передачи функций и/или полномочий по обслуживанию кредита и сбору задолженности любым третьим лицам), уступки, продажи, передачи в залог любым третьим лицам или обременения иным образом полностью или частично прав требования по договору и/или договору залога;

Для целей продвижения продуктов (услуг) банка на рынке, равно как продвижения совместных продуктов банка и/или продуктов (товаров, работ, услуг) третьих лиц - партнеров банка; на срок жизни клиента;

Как банку, так и любым третьим лицам, которые в результате обработки ПДн клиента, уступки, продажи, передачи в залог или обременения иным образом полностью или частично прав требования по договору и/или договору залога получили ПДн клиента, стали правообладателями (в качестве цессионария, покупателя, залогодержателя или бенефициара обременения) в отношении указанных прав, а также агентам и уполномоченным лицам банка и указанных третьих лиц.

Суд отметил, что в своем заявлении гражданка также выразила согласие на «обработку всех своих персональных данных банком любыми способами, в том числе третьими лицами, включая осуществление сбора, систематизацию, накопления, хранение, обновление, уточнение (проверка), изменение, использование и распространение (включая передачу), в том числе воспроизведение, электронное копирование и трансграничную передачу с целью выпуска, обслуживания кредитных карт, для создания информационных систем ПДнбанка, а также в целях предоставления информации третьим лицам, которые по договору с банком осуществляют деятельность по обеспечению погашения должниками просроченной задолженности».

Банк заключил договор с ООО «Эверест», согласно которому агентство оказывает ему услуги по взысканию задолженности, а банк предоставляет исполнителю по специальному запросу формы кредитных договоров, используемые заказчиком при предоставлении заемщикам различных видов кредитов, в отношении которых оказываются услуги (п. 3.1 данного договора).

По мнению суда, учитывая, что гражданка в своем заявлении дала банку разрешение на использование ПДн, предоставленных в целях заключения договора, и согласилась на их обработку банком различными способами, при этом информация по кредиту была доведена до нее при заключении кредитного договора надлежащим образом, то оснований для удовлетворения заявленных ею требований у суда не имелось.

Кроме того, судом первой инстанции не было установлено нарушение банком неприкосновенности частной жизни истца в нарушение положений ФЗ РФ от 27.07.2006 № 152-ФЗ «О персональных данных», а также не представлено доказательств, подтверждающих факт передачи ответиком ПДн об истце каким-либо иным третьим лицам.

Симоновский районный суд г. Москвы отказал в удовлетворении требований гражданина к АО Банк «Русский стандарт», ООО «Эверест» о обязании прекратить передачу персональных данных, взыскании морального вреда и судебных расходов.

Позиция Судебной коллегии по гражданским делам Московского городского суда

Судебная коллегия согласилась с выводами суда первой инстанции, отметив, что довод апелляционной жалобы гражданки о том, что 7 апреля 2015 года она направила в адрес банка заявление об отзыве своего разрешения на использование ПДн, которое было оставлено им без рассмотрения, не влечет отмену решения суда, так как согласия субъекта персональных данных на их обработку не требуется в случае, если обработка ПДн осуществляется в целях исполнения договора, одной из сторон которого является субъект ПДн.

Судебная коллегия оставил без изменения решение Симоновского районного суда г. Москвы, а апелляционную жалобу гражданки без удовлетворения.

Состав законодательства Республики Молдовы, отражающего вопросы защиты ПДн

Конституция Республики Молдовы в ст.28 предусматривает, что государство уважает и охраняет интимную, семейную и частную жизнь. Согласно ст. 30 Конституции государство обеспечивает тайну писем, телеграмм и других почтовых отправлений, телефонных переговоров и иных законных видов связи. Отступления от этих положений допускаются законом в случаях, когда это необходимо в интересах национальной безопасности, экономического благосостояния страны, общественного порядка и в целях предотвращения преступлений.

Неприкосновенность интимной, семейной и частной жизни относится к объектам гражданских прав и защищается всеми предусмотренными законом способами, прежде всего, в исковом порядке, путем возмещения причиненного морального вреда. Суды по заявлениям граждан присуждают им, как правило, сравнительно небольшие компенсации за причиненный моральный ущерб в связи с нарушением неприкосновенности частной жизни: распространением информации в СМИ, опубликованием личной переписки, раскрытием фактов личной жизни.

Законодательство страны в сфере обработки персональных данных, состоит, в том числе, из Конвенции Совета Европы о защите физических лиц при автоматизированной обработке данных личного характера, дополнительного протокола к этой Конвенции и других международных соглашений, стороной которых является Молдова. Республика Молдова подписала данную Конвенцию в мае 1998 года, ратифицировала ее постановлением Парламента в июле 1999 года. Конвенция вступила в силу для Молдовы с 1 июня 2008 года.

Вместе со сдачей на хранение ратификационной грамоты Конвенции, были представлены декларации, в которых власти заявили, что не будут применять Конвенцию в отношении обработки персональных данных физическими лицами исключительно для личных и семейных нужд (с условием, что они не нарушают права субъектов персональных данных), а также в отношении обработки персональных данных, относящихся к информации, являющейся государственной тайной. В то же время было заявлено, что Конвенция будет применяться в отношении персональных данных, которые не подвергаются автоматизированной обработке. Кроме того, Молдова назначила Национальный центр по защите персональных данных в качестве компетентного органа по исполнению положений Конвенции и поддержанию отношений взаимопомощи с другими государствами-участниками.

В апреле 2010 года был подписан, а в сентябре 2011 года ратифицирован Дополнительный протокол к Конвенции о защите физических лиц при автоматизированной обработке данных личного характера, касающийся органов контроля и трансграничной передачи данных. Он вступил в силу для Республики Молдова с 1 января 2012 года.

Действующий Закон о защите персональных данных был принят Парламентом в 2011 г. Закон вступил в силу в апреле 2012 г., его целью стало обеспечение защиты основных прав и свобод физического лица при обработке его персональных данных, в особенности права на неприкосновенность интимной, семейной и частной жизни. Им регулируются правоотношения, возникающие при обработке персональных данных полностью или частично автоматизированными средствами, а также при обработке средствами, отличными от автоматизированных, персональных данных, составляющих часть системы учета или предназначенных для введения в такую систему.

Законом предусмотрены основные характеристики персональных данных. Персональные данные, являющиеся предметом обработки, должны:

- Обрабатываться корректно и в соответствии с положениями закона;
- Собираться для объявленных, явных и законных целей и в дальнейшем не обрабатываться каким-либо образом, несовместимым с этими целями. Дальнейшая обработка персональных данных в статистических целях или в целях исторических или научных исследований не является несовместимой с целью сбора при условии, что она происходит с соблюдением положений закона, в том числе касающихся уведомления Национального центра по защите персональных данных, а также с соблюдением гарантий при обработке персональных данных, предусмотренных нормами, регулирующими статистическую деятельность, историческое и научное исследование;
- Быть адекватными, относящимися к делу и не быть избыточными в отношении целей, для которых они собираются или в дальнейшем обрабатываются;
- Быть точными и – если необходимо – актуализироваться. Неточные или неполные данные, применительно к целям, для которых они собирались или для которых они впоследствии обрабатывались, должны удаляться или исправляться;
- Храниться в форме, позволяющей идентификацию субъектов персональных данных не долее, чем это необходимо для целей, для которых данные собирались и впоследствии обрабатывались. Хранение персональных данных более длительные сроки в статистических целях или в целях исторических или научных исследований производится с соблюдением гарантий при обработке персональных данных, предусмотренных нормами, регулирующими эти области, и только в течение срока, необходимого для достижения этих целей.

Обработка персональных данных осуществляется с согласия субъекта персональных данных. Согласие на обработку может быть отозвано субъектом в любой момент. Отзыв согласия не может иметь обратной силы. При недееспособности или ограниченной дееспособности субъекта персональных данных согласие на обработку дает в письменной форме его законный представитель. В случае смерти субъекта персональных данных согласие в письменном виде дают его наследники, если оно не было дано субъектом персональных данных при его жизни.

Не требуется согласия субъекта персональных данных в случае, если обработка персональных данных необходима:

- Для исполнения договора, в котором субъект персональных данных является стороной, или для принятия мер до заключения договора по его просьбе;
- Для выполнения, предусмотренного законом обязательства контролера;
- Для защиты жизни, физической целостности или здоровья субъекта персональных данных;
- Для выполнения задач, имеющих общественное значение или вытекающих из властных полномочий органа публичной власти, возложенных на контролера или третью сторону, которой персональные данные раскрыты;
- В целях обеспечения законных интересов контролера или третьей стороны, которой раскрыты персональные данные, кроме случаев, когда такие интересы перекрываются интересами или основными правами и свободами субъекта персональных данных;
- Для статистических целей либо целей исторических или научных исследований, при условии, что персональные данные останутся анонимными в течение всего периода обработки.

Закон предусматривает закрытый перечень случаев, в которых могут обрабатываться особые категории персональных данных (для ряда категорий персональных данных предусмотрено специальное регулирование). Обработка особых категорий персональных данных запрещается, за исключением случаев, когда:

- Субъект персональных данных дал свое согласие. В случае недееспособности или ограниченной дееспособности субъекта персональных данных обработка особых категорий персональных данных возможна только при наличии письменного согласия его законного представителя;
- Обработка необходима в целях исполнения обязательств или особых прав контролера в сфере трудового права, при условии, что она осуществляется с соблюдением предусмотренных законом гарантий, а также с учетом

того, что любое раскрытие третьим сторонам персональных данных, обработанных для этих целей, может проводиться лишь при наличии соответствующего законного обязательства контролера;

- Обработка необходима для защиты жизни, физической целостности или здоровья субъекта персональных данных либо иного лица, если субъект персональных данных физически или юридически неспособен дать свое согласие;
- Обработка осуществляется в ходе законной деятельности общественными объединениями, партиями и другими общественно-политическими организациями, профсоюзами, объединениями работодателей, философскими или религиозными организациями, некоммерческими кооперативными организациями, при условии, что обработка относится исключительно к членам таковых или лицам, имеющим регулярные контакты с таковыми в связи с их целями, и что данные не раскрываются третьим сторонам без согласия субъекта персональных данных;
- Обработка относится к данным, добровольно и явно сделанным общедоступными субъектом персональных данных;
- Обработка необходима для определения, осуществления или защиты права субъекта персональных данных в суде;
- Обработка необходима в целях обеспечения безопасности государства, при условии, что она происходит с соблюдением прав субъекта персональных данных и других предусмотренных законом гарантий.

Трансграничная передача персональных данных, которые являются предметом обработки или подлежат обработке после передачи, возможна с разрешения Национального центра по защите персональных данных и лишь в том случае, если государство назначения обеспечивает адекватный уровень защиты прав субъектов персональных данных и данных, предназначенных для передачи. Уровень защиты определяется Национальным центром по защите персональных данных с учетом ряда условий, в том числе природы персональных данных, цели и продолжительности их обработки, государства назначения, его законодательства, а также профессиональных норм и мер безопасности в государстве назначения. Если Центр придет к выводу, что уровень защиты неудовлетворителен, он запрещает передачу данных.

Ограничения не действуют, если передача персональных данных происходит на основе специального закона или ратифицированного Молдовой международного договора, в частности, если речь идет о предотвращении или расследовании преступлений. При этом специальный закон или международный договор должны предусматривать гарантии защиты прав субъектов персональных данных. Особое регулирование применяется и в случае обработки

персональных данных исключительно в целях журналистики, художественного или литературного творчества, если обрабатываются данные, добровольно и явно сделанные общедоступными субъектом персональных данных либо тесно связанные со статусом публичной фигуры субъекта персональных данных или публичным характером действий, в которые он вовлечен.

Закон допускает передачу персональных данных в государства, не обеспечивающие адекватный уровень защиты, только в следующих случаях:

- Наличие согласия субъекта персональных данных;
- Необходимость заключения или исполнения соглашения, или договора между субъектом персональных данных и контролером либо между контролером и третьей стороной в интересах субъекта персональных данных;
- Если это необходимо для защиты жизни, физической целостности или здоровья субъекта персональных данных;
- Если передача производится из регистра, который предназначен для информирования общественности и который открыт для ознакомления либо общественности в целом, либо любому лицу, проявляющему законный интерес, в той мере, в какой условия, предусмотренные законом для ознакомления, выполняются в конкретном случае;
- Если это необходимо для удовлетворения важного общественного интереса, такого как национальная оборона, госбезопасность или общественный порядок, для нормального хода уголовного судопроизводства либо определения, осуществления или защиты права в суде, при условии, что персональные данные обрабатываются в связи с этими целями и только в течение срока, необходимого для достижения этих целей.

Судебные случаи по тематике «Трансграничная передача ПДн»

30 марта 2016 г.

Дорогомиловский районный суд г. Москвы в составе: председательствующего судьи Шипиковой А.Г., при секретаре Адиятуллиной А.Р., рассмотрев в открытом судебном заседании гражданское

дело № 2-220/2016

по иску М******* Г******* Н******* к АО «*******» о предоставлении информации, компенсации морального вреда и судебных расходов,

УСТАНОВИЛ:

М******* Г.Н. обратилась в суд с иском к АО «*******» о предоставлении информации, касающейся обработки персональных данных, компенсации морального вреда в размере 20 000 руб., взыскании расходов на представителя в размере 5 000 руб. и государственной пошлины в размере 300 руб.

В обоснование иска истец указала, что между сторонами заключен договор о выпуске и обслуживании кредитной карты путем присоединения заемщика к Условиям кредитования и подписания Заявления - Анкеты, в соответствии с которыми истцу Банком предоставлена кредитная карта № *******.

Договор включал в себя в качестве неотъемлемых частей Общие условия выпуска и обслуживания кредитных карт Банка, входящие в состав Условий комплексного банковского обслуживания в Банке, Тарифы и Заявление-Анкету, содержащие информацию о паспортных данных истца и месте регистрации.

15 июня 2015 г. истец направила в адрес Банка заявление о предоставлении информации, касающейся обработки персональных данных, предоставленных в рамках Договора о выпуске и обслуживании кредитной карты, а именно: подтвердить факт обработки персональных данных, сообщить правовые основания и цели обработки персональных данных, сообщить наименование и сведения о лицах, которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с АО «*******», сообщить наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению АО «*******».

До настоящего времени запрашиваемая информация истцу не предоставлена, что нарушает права истца.

Незаконными действиями банка истцу причинен моральный вред, который она оценивает в 20 000 руб.

Истец М******* Г.Н. в судебное заседание не явилась, извещалась надлежащим образом телеграммой, сведения о дате и времени судебного заседания размещены на сайте Дорогомиловского районного суда г. Москвы, в исковом заявлении обратилась о рассмотрении дела в ее отсутствие.

Представитель АО «*******» в судебное заседание не явился, извещен надлежащим образом телеграммой, в материалы дела представлены письменные возражения на иск.

Дело рассмотрено в отсутствие сторон в порядке ст. 167 ГПК РФ.

Суд, исследовав письменные материалы дела, находит иск

подлежащим отказу по следующим основаниям.

В соответствие со ст. 6 Федерального закона «О персональных данных», обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем.

В соответствии с ч. 7 ст. 14 Федерального закона «О персональных данных», субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей: подтверждение факта обработки персональных данных оператором; правовые основания и цели обработки персональных данных; цели и применяемые оператором способы обработки персональных данных; наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона; обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом; сроки обработки персональных данных, в том числе сроки их хранения; порядок осуществления субъектом персональных данных прав, предусмотренных настоящим Федеральным законом; информацию об осуществленной или о предполагаемой трансграничной передаче данных; наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу; иные сведения, предусмотренные настоящим Федеральным законом или другими федеральными законами.

В соответствии с ч. 1 ст. 20 Федерального закона «О персональных данных», оператор обязан сообщить в порядке, предусмотренном статьей 14 настоящего Федерального закона, субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя либо в течение тридцати дней с даты получения запроса субъекта персональных данных или его представителя.

В соответствии с ч. 1 ст. 17 Федерального закона «О персональных данных», если субъект персональных данных считает, что оператор осуществляет обработку его персональных данных с нарушением требований Федерального закона или иным образом нарушают его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

Судом установлено, ******* 2012 г. между М******* Г.Н. и АО «*******» был заключен договор о предоставлении и обслуживании кредитной карты № *******.

Составными частями заключенного договора являются Заявление-Анкета, подписанная истцом, Тарифы по тарифному плану, указанному в Заявлении- Анкете, Общие условия выпуска и обслуживания кредитных карт ТКС Банка (ЗАО).

При заключении Договора кредитной карты в Заявлении-анкете, истец выразила свое согласие на обработку всех своих персональных данных Банком любыми способами, в том числе третьими лицами, включая осуществление сбора, систематизацию, накопление, хранение, обновление, уточнение (проверка), изменение, использование и распространение (включая передачу), в том числе воспроизведение, электронное копирование и трансграничную передачу … с целью выпуска, обслуживания кредитных карт, для создания информационных систем персональных данных Банка, в целях предоставления информации третьим лицам, которые по договору с Банком осуществляют деятельность по обеспечению погашения должниками просроченной задолженности.

Таким образом, Банк при заключении Договора получил согласие истца на обработку персональных данных в соответствии с требованием вышеуказанного Федерального закона «О персональных данных».

******* 2015 г. истец обратилась в Банк с требованием предоставить информацию, касающуюся обработки персональных данных.

Банк в соответствии со ст. 20 Федерального закона «О персональных данных» ******* 2015 г. направил истцу ответ на заявление от ******* 2015 г.

При таких обстоятельствах, учитывая, что Банк дал ответ на заявление истца, права М******* Г.Н. не нарушены.

Кроме того, истец в силу ст. 56 ГПК РФ не представила суду доказательств, подтверждающих факт нарушения Банком порядка обработки ее персональных данных.

Суд также учитывает, что требования М******* Г.Н. об обязании предоставить ей информацию о лицах, допущенных к обработке ее персональных данных, включая фамилию, имя, отчество и адрес не основаны на положениях ч. 7 ст. 14 Федерального закона «О персональных данных».

Учитывая, что банком не допущено нарушения прав истца как потребителя и заемщика, морально-нравственные страдания М******* Г.Н. причинены не были, порядок обработки персональных данных истца Банком не нарушался, оснований для компенсации морального вреда не имеется.

На основании изложенного, руководствуясь ст.ст.194-199 ГПК РФ, суд

ПОСТАНОВИЛ

В удовлетворении иска М******* Г******* Н******* к АО «*******» о предоставлении информации, компенсации морального вреда и судебных расходов - отказать.

Решение суда может быть обжаловано в Московский городской суд через Дорогомиловский районный суд г. Москвы в апелляционном порядке в течение месяца со дня изготовления мотивированного решения.

Судья: Шипикова А.Г.

Состав законодательства Республики Беларусь в области защиты ПДн

В соответствии с законом Республики Беларусь от 10.11.2008 N 455-З (ред. от 11.05.2016) "Об информации, информатизации и защите информации" (далее – Закон об информации), персональные данные - основные и дополнительные персональные данные физического лица, подлежащие в соответствии с законодательными актами Республики Беларусь внесению в регистр населения, а также иные данные, позволяющие идентифицировать такое лицо. Персональные данные относится к информации, распространение и предоставление которой ограничено.

Закон Республики Беларусь от 21.07.2008 N 418-З (ред. от 04.01.2015) "О регистре населения" (далее – Закон о регистре населения) определяет следующие основные персональные данные: идентификационный номер, фамилия, собственное имя, отчество, пол, число, месяц, год рождения, место рождения, цифровой фотопортрет, данные о гражданстве (подданстве), данные о регистрации по месту жительства и (или) месту пребывания, данные о смерти или объявлении физического лица умершим, признании безвестно отсутствующим, недееспособным, ограниченно дееспособным.

Дополнительными персональными данными, в соответствии с Законом о регистре населения, являются: данные о родителях, опекунах, попечителях, семейном положении, супруге, ребенке (детях) физического лица, о высшем образовании, ученой степени, ученом звании, о роде занятий, о налоговых обязательствах и некоторые иные.

Отдельная статья Закона «Об информации» посвящена мерам по защите персональных данных от разглашения. Так, в соответствии со статьей 32 такие меры должны быть приняты с момента, когда персональные данные были предоставлены физическим лицом, к которому они относятся, другому лицу либо когда предоставление персональных данных осуществляется в соответствии с законодательными актами Республики Беларусь. Последующая передача персональных данных разрешается только с письменного согласия физического лица, к которому они относятся, либо в соответствии с законодательными актами Республики Беларусь.

Меры по защите персональных данных от разглашения должны приниматься до:

- уничтожения персональных данных, либо до

- их обезличивания, либо до
- получения письменного согласия физического лица, к которому эти данные относятся, на их разглашение.

Под защитой персональных данных, содержащихся в регистре, в соответствии со статьей 31 Закона «О регистре» понимается деятельность распорядителя регистра, направленная на предотвращение несанкционированного вмешательства в процесс ведения регистра, в том числе попыток незаконного доступа к персональным данным, содержащимся в регистре, их блокирования, копирования, предоставления, распространения, искажения, уничтожения, а также иных неправомерных действий в отношении этих персональных данных.

Таким образом в законодательстве Республики Беларусь определены лишь базовые положения, направленные на создание механизма защиты персональных данных. В белорусских законодательных актах не содержится положений, которые включали бы все принципы защиты персональных данных, перечисленные в 108 Конвенции Совета Европы.

Состав законодательства Испании, отражающего вопросы защиты ПДн

Сегодня поговорим об одном из важнейших законов – Законе о защите персональных данных (Ley de Protección de Datos (LOPD)), о его исполнении и о том, как закон влияет на работу предпринимателей и компаний малого и среднего бизнеса в Испании. Не обойдем вниманием и последнее нововведение – Основной регламент о защите персональных данных (Reglamento General de Protección de Datos (RGPD)), вступивший в силу и наделавший немало шума.

Предприниматели и компании обязаны соблюдать Закон о защите персональной информации (далее – LOPD), если в процессе своей деятельности они ведут сбор личных данных. В данном случае под «личными данными» понимаются те, которые позволяют идентифицировать физическое лицо.

Для того, чтобы должным образом соблюсти все требования LOPD, необходимо понимать:

- Цели LOPD
- Почему необходимо исполнять LOPD
- Как исполнять LOPD
- Основной регламент о защите персональных данных — Reglamento General de Protección de Datos(RGPD)

25 мая 2016 года вступил в силу Основной регламент о защите персональных данных (далее – RGPD), который обязал предпринимателей и юридических лиц внести определенные изменения в свою политику защиты персональных данных. На эту процедуру было отведено два года, т.е. с 25 мая 2018 года закон должен целиком и полностью исполняться во всех без исключения странах-членах ЕС. В ближайшем будущем ожидается выход нового закона — Ley de Protección de Datos de Carácter Personal, – проект которого уже находится на рассмотрении. Ожидается, что закон приведет все нормативы в соответствие с европейским регламентом.

Цели LOPD

Основной целью закона является гарантия защиты и надлежащей обработки данных, носящих персональный характер. Эти данные принято делить на три уровня:

- Базовый уровень: идентификационные данные — (ИНН (NIF), номер социального страхования, имя, фамилия, адрес, номер телефона, подпись, личное фото, адрес электронной почты, имя пользователя, номер банковской карты, номерной знак машины и т.д.

- Средний уровень: данные, касающиеся административных или уголовных правонарушений, платежеспособности и кредитоспособности, фискальные данные, данные, связанные с социальным страхованием, получением финансовых продуктов, а также те, в которых отражаются личные предпочтения, привычки, склонности и т.д.
- Высший уровень: данные о личной идеологии, религии, мировоззрении, расовой принадлежности, здоровье, сексуальных пристрастиях или гендерном насилии.

Ответственность за использование и хранение этих данных несет лицо, которое их получило. На него же возлагается ответственность по соблюдению всех требований, предписанных LOPD.

В частности, ответственное лицо обязано:

- Регистрировать учетные базы данных в соответствии с Главным реестром защиты персональных данных.
- Контролировать качество данных, и адекватность и достоверность.
- Обеспечивать секретность, гарантировать безопасность данных.
- Информировать и получать согласие на получение и обработку персональных данных.
- Уважать права граждан в части доступа, изменения, отзыва, удаления и оспаривания своих персональных данных.

Иными словами, LOPD призван обеспечить неприкосновенность и защиту персональных данных физических лиц. Однако подобная защита не распространяется на юридические лица. Таким образом, предприниматель может как попадать под защиту, так и не попадать, в зависимости от ситуации, в которой находится:

Предприниматель-управляющий ООО (S.L.) или АО (S.A.): не обязан лично нести ответственность за защиту персональных данных клиентов, т.к. в данном случае обязанность возлагается целиком и полностью на компании. И, тем не менее, предприниматель-управляющий обязан следить за надлежащим исполнением LOPD.

Независимый предприниматель, имеющий наемных работников: отвечает за безопасность персональных данных своих работников, а также поставщиков и клиентов.

Независимый предприниматель, не имеющий наемных работников: необходимо оценить характер деятельности предпринимателя и понять, ведется ли сбор персональных данных клиентов и поставщиков, и если да, то какого типа данные собираются. Если база персональных данных отсутствует, то, соответственно не возникает никаких обязательств

по соблюдению LOPD. Однако если клиентами предпринимателя являются частные лица, то, вероятнее всего, исполнять закон придется.

Почему необходимо исполнять LOPD

В первую очередь, для того, чтобы подтвердить, что наш бизнес соблюдает все действующие нормы законодательства. Любая потеря конфиденциальных данных по причине технических сбоев, пожара, наводнения и т.п., может обернуться немалыми потерями для компании, т.к. в данном случае мы начинаем говорить о гражданской ответственности, недобросовестной конкуренции и т.п. Не стоит забывать и о возможных экономических санкциях против компании, т.е. затраты на внедрение системы исполнения LOPD могут оказаться незначительными, если сравнить их с возможными негативными последствиями в случае пренебрежения и неисполнения закона.

Согласно нормам действующего законодательства, к нарушителю могут применяться следующие санкции:

- За легкие нарушения – штраф от 900 до 40.000 €.
- За тяжкие нарушения – штраф от 40.001 до 300.000 €.
- За очень тяжкие нарушения – штраф от 300.001 до 600.000 €.

Степень правонарушения определяется в зависимости от типа данных, которых оно коснулось: базовый уровень, средний уровень или высший уровень. В определении суммы штрафа используются следующие критерии:

- Продолжительность нарушения.
- Объем данных.
- Связь между деятельностью нарушителя и обработкой персональных данных.
- Объемы деятельности нарушителя.
- Выгода, напрямую вытекающая из нарушения.
- Степень нарушения.
- Повторные нарушения аналогичного характера.
- Характер причиненного вреда.

Возможно, будет установлено, что со стороны ответственного лица не было совершено никаких нарушений, что обработка и хранение данных велись с соблюдением всех действующих норм и требований, а причиной нарушения

послужила аномалия, а не халатность и не пренебрежение своими обязанностями ответственным лицом. Любые иные обстоятельства будут учитываться в определении степени вины ответственной стороны.

Помимо штрафов предусмотрены также выговоры, если речь идет о легких или тяжких нарушениях, и если ранее нарушитель не привлекался к ответственности и не был замечен в подобных нарушениях. Испанское агентство по защите персональных данных праве потребовать исправить выявленные нарушения, не инициируя судебное разбирательство.

Как исполнять LOPD

Обработка данных может проходить под контролем Испанского агентства по защите персональных данных (AEPD — Agencia Española de Protección de Datos), отвечающего за соблюдение нормативов и гарантирующего фундаментальное право граждан на защиту персональных данных. Но можно также довериться специалисту, который возьмет на себя труд пройти все необходимые бюрократические процедуры. Процесс внедрения LOPD включает:

- Идентификация учетных карточек, содержащих персональные данные работников, клиентов, поставщиков и т.д.
- Определение уровня безопасности.
- Идентификация управляющего учетными карточками.
- Разработка документации о безопасности.
- Обучение лица, ответственного за учетные карточки.
- Уведомление владельцев данных о наличии учетных карточек.
- Регистрация учетных карточек в реестре Испанского агентства по защите персональных данных.

Если компания ведет сбор данных среднего и высшего уровней, она обязана проводить аудит. Аудит необходим также в случае изменений в информационной системе, способных так или иначе затронуть персональные данные третьих лиц. Аудит может быть внешним и внутренним и заканчиваться выдачей заключения о соответствии или несоответствии компании действующим нормам законодательства. В случае несоответствия указываются недостатки и рекомендации по их устранению.

Заключение должно быть проверено лицом, ответственным за безопасность, и передано лицу, ответственному за учетные карточки, которое, в свою очередь, должно принять решение о выборе и принятии необходимых мер. Заключение в итоге передается в распоряжение AEPD и контролирующих органов автономии.

Основной регламент о защите персональных данных — Reglamento General de Protección de Datos (RGPD)

Этот норматив уже вступил в силу и распространяется на всех жителей ЕС. Основной целью регламента является улучшение процесса и упрощение бюрократических процедур. Компании получают чуть больше обязанностей по обработке и защите персональных данных. Предприниматели и компании малого и среднего бизнеса до 25 мая 2018 года обязаны сделать следующее:

- Обеспечить получение четкого и ясного согласия (а не согласия по умолчанию) клиентов на использование их персональных данных.
- Обновить положения политики защиты персональных данных.
- В обязательном порядке назначить внутреннего или внешнего уполномоченного по защите данных.
- Запустить оценку воздействия защиты персональных данных (PIA).
- Ввести новый алгоритм обеспечение безопасности персональных данных.
- Получить сертификат об исполнении RGPD.

В течение 72 часов уведомить контролирующие органы о выявленных нарушениях в процедуре защиты персональных данных.

Судебные случаи по тематике «Трансграничная передача ПДн».

Решение Суда Европейского Союза по иску против Facebook. Суд Европейского Союза принял решение [1], которое может привести к тому, что передача персональных данных из Европы в США будет признана противоречащей требованиям законодательства ЕС о защите персональных данных [2]. Это решение было принято 6 октября 2015 года на основании обращения австрийского юриста Maximilian Schrems, аспиранта Венского Университета, в Ирландский суд с жалобой против Facebook. Он жаловался, что Facebook хранит его персональные данные в США, включая те, которые он удалил со своей страницы, и тем самым нарушает его права на охрану персональных данных. В качестве аргумента о существовании угрозы Максимилиан Шремс ссылался на признание Эдварда Сноудена о том, что американские спецслужбы получали информацию о гражданах от Google, Apple и Facebook.

Ирландский суд передал на рассмотрение Суду Европейского Союза вопрос о том, нарушаются ли права пользователей при передаче их персональных данных в США.

В Еропейском Союзе действует директива о защите персональных данных [3], которая предусматривает, что персональные данные могут передаваться в другие страны, если при этом в стране, куда они передаются, обеспечивается определенный уровень их защиты. Вопрос о том, обеспечивается ли защита персональных данных в конкретной стране, может решаться Комиссией ЕС. Но следить за соблюдением требований директивы должны специально уполномоченные органы каждого государства – члена ЕС.

июле 2000 года Комиссия ЕС приняла решение, что в США обеспечивается требуемый уровень защиты персональных данных – так называемое Safe Harbour Decision [4]. Причем в этом решении Комиссии говорится, что американские компании, которые сами себя сертифицируют на основании safe harbor program, обеспечивают необходимую защиту персональных данных.

В своем решении Суд ЕС указал, что указанные выводы Комиссии никак не влияют на обязанности специально уполномоченных органов в государствах-членах ЕС следить за охраной персональных данных. И более того, решение Комиссии не является обязательным для этих органов. Но при этом Суд также рассмотрел и само решение Комиссии и признал его недействительным. Выводы Суда базируются на том факте, что на самом деле Комиссия, принимая решение

Safe Harbour Decision, не изучала положения законодательства США на предмет охраны персональных данных. Кроме того, safe harbor program, которую обязывались соблюдать компании, никак не влияет на действия государственных органов США. На самом деле власти США имеют возможность почти неограниченного доступа к персональным данным. Вторым аргументом Суда стал тот факт, что законодательством США не предусматривает возможность обращений пользователей с просьбой изменить их данные или удалить их, если они являются не точными или недостоверными. Все это идет в разрез с двумя требованиями законодательства Европейского Союза: об охране персональных данных и об обеспечении доступа к правосудию.

Европейское ИТ сообщество очень встревожено этим решением. Некоторые комментаторы даже заявили, что около 4.400 европейских компаний, хранящих данные европейских пользователей на американских серверах, должны срочно решить как переместить все эти данные на другую территорию. Также указываются большие суммы потерь в связи с этим: 1,3% ВВП Европейского Союза [5]. Но на самом деле это не совсем так.

Пока что единственное, что последует за решением Суда ЕС, это то что вопрос о том, может ли Facebook передавать персональные данные европейских пользователей в США, будет рассмотрен специально уполномоченным органом в Ирландии. И уже на основании этого административного решения компании, передающие персональные данные в США, могут начать беспокоиться о передаче данных. Но формально, решение ирландских властей не будет угрожать компаниям из других стран ЕС. Хотя в долгосрочной перспективе можно представить себе постепенное признание Европейским Союзом ненадежности США для хранения персональных данных пользователей. Но что последует после этого спрогнозировать практически не возможно: в борьбе интересов спец служб и крупнейших ИТ компаний, как Facebook, исход не ясен.

В общем, вопрос о хранении и локализации персональных данных в последнее время становится все более актуальным во многих странах. В России с 1 сентября 2015 года действует требование о хранении персональных данных на серверах, расположенных на территории России. Хотя, как всегда, вопросов больше, чем ответов. Например, как доказать трансграничную передачу данных в нарушение требования о локализации? Очевидно, что в ближайшие годы вопросы, связанные с персональными данными, будут крайне актуальными. Не спроста же говорят, что “personal data is the new oil of XXI century”.