

Одно из актуальных направлений внутреннего контроля — контроль соблюдения законодательства о персональных данных (ПДн), в частности соответствия внутренних документов законодательству о ПДн. Какие основные нарушения в области сбора и обработки ПДн в 2017 году стали причиной привлечения банков к административной ответственности? Что признается избыточной обработкой ПДн? Какие локальные акты необходимо разработать в банке, учитывая, что законодательство не содержит перечня обязательных внутренних документов по работе с ПДн?

Вячеслав ЧМЫХОВ, юридическая фирма VEGAS LEX, юрист Коммерческой группы

Татьяна ДВЕНАДЦАТОВА, юридическая фирма VEGAS LEX, юрист Группы международных проектов

Контроль работы с персональными данными: нарушения и методы их предотвращения



Тема регулирования и защиты ПДн с каждым годом становится все актуальнее, сохраняя при этом определенную долю специфики в зависимости от направления деятельности оператора ПДн. Наиболее яркими примерами нарушений в банковской отрасли можно считать случаи утечки баз данных, содержащих ПДн субъектов, а также участвовавшие факты несанкционированной передачи ПДн финансовыми организациями третьим лицам.



В последнем случае типичной иллюстрацией может служить практика передачи кредитными организациями информации о задолженности и должнике коллекторским агентствам. Закон № 353-ФЗ¹ допускает передачу ПДн заемщика и лиц, выступивших поручителями, третьим лицам при уступке прав (требований) по договору потребительского кредита (займа). Однако кредитные организации нередко оставляют нормы Закона № 353-ФЗ без внимания и передают данные заемщика третьим лицам без получения согласия субъекта ПДн.

¹ Федеральный закон от 21.12.2013 № 353-ФЗ «О потребительском кредите (займе)».

Контроль работы с персональными данными: нарушения и методы их предотвращения

С появлением законодательства, регулирующего деятельность по возврату просроченной задолженности¹, требования к коллекторским агентствам стали жестче, однако есть сомнения, что специальный закон сможет в один момент устранить все проблемы с ПДн.

Стоит отметить, что положительная статистика в области соблюдения бизнесом законодательства о ПДн все же просматривается. Так, объем штрафов, наложенных Роскомнадзором по итогам проверок, снизился с 10,5 млн руб. в 2015 г. до 6 млн руб. в 2016 г. Количество выявленных нарушений и выданных Роскомнадзором предписаний по сравнению с 2014 и 2015 гг. также снизилось. Это свидетельствует о том, что бизнес-сообщество стало приспосабливаться к ужесточившимся требованиям законодательства о ПДн. Скорее всего, такая тенденция сохранится и в будущем, учитывая вступившие в силу 1 июля 2017 г. поправки в КоАП РФ (ст. 13.11), которыми были существенно изменены положения, устанавливающие ответственность за нарушение законодательства в области ПДн.

Тем не менее, несмотря на общую положительную тенденцию, на конец 2016 г. наибольшее количество жалоб граждан поступило на действия кредитных учреждений (преимущественно связанные с передачей ПДн без согласия граждан), что в первую очередь обусловлено обработкой ими ПДн значительного числа граждан.

Итак, что необходимо принимать во внимание службе внутреннего контроля кредитной организации, оценивая степень соблюдения законодательства о ПДн?

Основные понятия и применимое законодательство

Регулирование отношений, связанных с обработкой ПДн с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, или без использования таких средств, осуществляется на базе Закона № 152-ФЗ².

Вместе с тем регулирование ПДн в российском праве осуществляется с применением ряда других нормативно-правовых актов, включая Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Трудовой кодекс РФ. Не стоит упускать из вида и ведомственные акты,

¹ Федеральный закон от 03.07.2016 № 230-ФЗ «О защите прав и законных интересов физических лиц при осуществлении деятельности по возврату просроченной задолженности и о внесении изменений в Федеральный закон “О микрофинансовой деятельности и микрофинансовых организациях”».

² Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

Вячеслав ЧМЫХОВ Татьяна ДВЕНАДЦАТОВА

которые касаются наиболее специфичных вопросов в сфере обработки ПДн¹.

Понятие ПДн является одним из центральных понятий, содержащихся в действующем законодательстве. Статья 3 Закона № 152-ФЗ определяет персональные данные как любую информацию, относящуюся к прямо или косвенно определенному или определяемому физическому лицу (субъекту ПДн). Интересно, что в Общем регламенте Европейского союза о защите персональных данных² ПДн толкуются как «любая информация, относящаяся к идентифицированному или идентифицируемому физическому лицу (“субъекту данных”)», а определяемое лицо толкуется как «лицо, которое может быть идентифицировано прямо или косвенно, в частности посредством таких идентификаторов, как имя, идентификационный номер, сведения о местоположении, идентификатор в режиме онлайн, или через один или несколько признаков, характерных для физической, психологической, генетической, умственной, экономической, культурной или социальной идентичности указанного физического лица».

В сравнении с российским европейский законодатель выработал более конкретный подход и указал ряд формальных критериев, необходимых для квалификации информации в качестве персональных данных.

В сравнении с российским европейский законодатель выработал более конкретный подход и указал ряд формальных критериев, необходимых для квалификации информации в качестве ПДн³. Возможность идентификации любого живого лица должна быть основана на конкретной информации. По аналогичному пути пошел и российский правоприменитель.

Так, обзор разъяснений Роскомнадзора и судебной практики позволяет сделать вывод, что ключевым аспектом является способность идентифицировать лицо с помощью таких данных. Поскольку Закон № 152-ФЗ не уточняет, что именно на базе таких данных лицо может быть установлено/определено, в судебной практике нередко возникают вопросы, что следует относить к ПДн субъекта.

Например, часто возникают споры относительно того, можно ли считать IP-адрес персональными данными, ведь IP-адрес позволяет

¹ См., например, Указ Президента РФ от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера», Приказ ФСБ России и ФСТЭК России от 31.08.2010 № 416/489 «Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования», Приказ Роскомнадзора от 15.03.2013 № 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» и др.

² Регламент (ЕС) № 2016/679 Европейского Парламента и Совета ЕС «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене директивы 95/46/ЕС (Общий регламент о защите персональных данных)».

³ О новых тенденциях в европейском регулировании защиты ПДн и об их влиянии на международную деятельность российских банков см. также: Дроздов А. Новое законодательство ЕС о защите персональных данных: возможные последствия // Международные банковские операции. 2017. № 1.

Контроль работы с персональными данными: нарушения и методы их предотвращения

идентифицировать устройство, с которого был осуществлен выход в интернет, но никак не конкретного пользователя¹. Хотя Суд Европейского союза, например, заявляет, что IP-адреса являются охраняемыми ПДн², российские суды не так категоричны и прямо не указывают в своих решениях на то, что IP-адрес можно отнести к ПДн.

Однако совершенно очевидно, что в подавляющем большинстве случаев с помощью IP-адресов можно идентифицировать устройство, с которого выполнялся выход в интернет, и круг пользователей, а также их взаимосвязь, если пользователи выходили в сеть с одного IP-адреса³.

Понятие *оператора персональных данных* также нуждается в пояснении. Оператором ПДн признается лицо, которое самостоятельно или совместно с другими лицами организует или осуществляет обработку ПДн, а также определяет цель обработки, состав подлежащих обработке ПДн и круг действий, совершаемых с ПДн. Оператор ПДн несет ответственность за нарушение прав субъекта ПДн при их обработке.

Понятие *обработки персональных данных* включает в себя любое действие/операцию или совокупность действий/операций, совершаемых с использованием средств автоматизации или без использования таких средств с ПДн. Содержание и объем обрабатываемых ПДн должны полностью соответствовать заявленным целям обработки.

Российские суды указывают, что IP-адрес можно отнести к персональным данным.

Практический обзор основных нарушений в области персональных данных

Банки в основном допускают следующие нарушения в области персональных данных:

- ненадлежащее обеспечение сохранности и конфиденциальности данных;
- избыточная обработка данных или несоответствие обработки заявленным целям;
- ненадлежащее оформление согласия субъекта ПДн на обработку данных.

¹ См. подробнее судебную практику, где суды не признали IP-адрес персональными данными: Постановление Тринадцатого арбитражного апелляционного суда от 05.07.2017 № 13АП-5614/2017, 13АП-5604/2017 по делу № А56-12177/2016.

² См.: Judgment of the Court (Third Chamber) 24 November 2011 in Case C-70/10 (<http://curia.europa.eu/juris/document/>).

³ См. Постановления Третьего арбитражного апелляционного суда от 08.09.2017 по делу № А74-13090/2016, Восьмого арбитражного апелляционного суда от 05.09.2017 № 08АП-7948/2017 по делу № А75-16756/2016.

Вячеслав ЧМЫХОВ Татьяна ДВЕНАДЦАТОВА

Рассмотрим перечисленные составы правонарушений на примере судебных решений.

Обеспечение сохранности и конфиденциальности данных

Наиболее распространены нарушения в области обеспечения сохранности ПДн, их конфиденциальности и законности передачи третьим лицам (преимущественно при уступке прав по договорам кредитования). Так, в типовые договоры кредитования банки зачастую включают безальтернативные условия о согласии субъекта ПДн на передачу его данных третьим лицам. Включение в договор условий о согласии на передачу ПДн является нарушением Закона № 152-ФЗ одновременно в части требований к письменной форме согласия и указания конкретного перечня третьих лиц, в отношении которых клиент дает такое согласие.

В частности, суды указывают на необходимость устанавливать в договоре наименование и адрес третьих лиц, которые позволят их идентифицировать, а также предоставлять субъекту право недвусмысленно выразить согласие или отказ в передаче его данных.

Так, крупнейший отечественный банк совсем недавно был привлечен к административной ответственности по ч. 1 и 2 ст. 14.8 КоАП РФ. Банк заключил с физическим лицом договор о потребительском кредите, который не содержал ярко выраженное альтернативное условие, предоставляющее лицу возможность согласиться на уступку банком прав требования по договору третьим лицам или отказаться от такой уступки. Пункт договора содержал безальтернативное условие об уступке прав требования по договору, а также не содержал конкретного перечня третьих лиц, которым впоследствии будут переуступлены права и переданы ПДн субъекта.

Апелляционный суд отказал банку в удовлетворении требования об оспаривании привлечения к ответственности, сделав вывод о том, что банк предоставил третьим лицам необоснованное право на обработку ПДн клиентов банка без получения предварительного согласия последних¹.

Аналогичным образом отечественная страховая организация, входящая в крупнейший российский банковский холдинг, была привлечена к административной ответственности по ч. 2 ст. 14.8 КоАП РФ. Обстоятельства дела заключались в том, что в страховом полисе содержался безальтернативный пункт о согласии потреби-

Банк может быть привлечен к ответственности за то, что договор о потребительском кредите не содержит ярко выраженное альтернативное условие, предоставляющее лицу возможность согласиться на уступку банком прав требования по договору третьим лицам или отказаться от такой уступки.

¹ Постановление Одиннадцатого арбитражного апелляционного суда от 27.11.2017 по делу № А65-16479/2017.

Контроль работы с персональными данными: нарушения и методы их предотвращения

теля на уступку прав по договору третьим лицам и на соответствующую обработку его данных третьими лицами. У лица отсутствовал выбор при предоставлении согласия, а кроме того, были нарушены требования Закона № 152-ФЗ об определении конкретного перечня лиц в согласии. Суд сделал вывод, что факт подписания договора клиентом страховой организации не является надлежащим доказательством предоставления гражданину возможности выразить согласие или отказаться от предоставления сведений третьим лицам: условия договора были разработаны таким образом, что у лица отсутствовала свобода выбора¹.

Аналогичные выводы судов содержатся во многих решениях, включая решения Арбитражного суда Самарской области от 23.08.2017 по делу № А55-6296/2017; Арбитражного суда г. Москвы от 13.09.2017 по делу № А40-102354/2017; Арбитражного суда г. Москвы от 23.10.2017 по делу № А40-13362/2017.

Избыточная обработка и ее несоответствие заявленным целям

В области избыточной обработки ПДн и обработки данных в нарушение целей, которые указаны в согласии субъекта, банки зачастую допускают нарушения, возлагая на субъект ПДн обязанность уведомлять об отдельных событиях и изменениях во время исполнения договора кредитования.

Так, банки стремятся быть в курсе любой информации, которая может негативно повлиять на способность заемщика исполнить обязательства по кредитному договору. В частности, они требуют сообщать информацию об изменении состава семьи, возбуждении уголовного дела, изменении места работы, адреса проживания и иную информацию. Суды приходят к выводу, что включение в договоры кредитования обязанности субъекта ПДн информировать банки о различных аспектах своей жизни нарушает действующее законодательство, поскольку сбор таких данных является избыточным и не влияет на существо кредитных отношений. До заключения договора банк имеет законную возможность запросить всю необходимую информацию и в отдельных случаях отказаться от кредитования.

Так, отечественный банк был привлечен к административной ответственности по ч. 2 ст. 14.8 КоАП РФ. В одном из пунктов кредитного договора было прописано, что заемщик обязан уведомить кредитора о заключении (об изменении) брачного договора, об изме-

Условия договоров, предписывающие уведомлять кредитора об изменении адреса регистрации (прописки), места работы, паспортных данных (замене паспорта), ущемляют права потребителя.

¹ Решение Арбитражного суда г. Москвы от 23.11.2017 по делу № А40-174258/2017.

Вячеслав ЧМЫХОВ Татьяна ДВЕНАДЦАТОВА

нении состава семьи, работы или места жительства, о смене фамилии и об иных данных, позволяющих идентифицировать субъекта. Суд пришел к выводу, что соответствующий пункт кредитного договора ущемлял права потребителя установлением обязанности предоставлять в банк персональную информацию, обязательность предоставления которой не установлена законодательством РФ и не влияет на исполнение целей кредитного договора¹.

Похожие выводы содержатся в Постановлении Седьмого арбитражного апелляционного суда от 25.08.2017 по делу № А27-4649/2017. Так, суд подтвердил правомочность привлечения к административной ответственности крупного банка, проверка типовых договоров которого выявила необоснованное включение положений о праве кредитора запросить у заемщика всю необходимую информацию. Позиция суда заключалась в том, что действующее законодательство не предусматривает обязанности заемщика-гражданина после получения займа уведомлять кредитора о возникновении или об изменении любых обстоятельств, способных повлиять на выполнение обязательств по договору, поскольку это не может являться основанием для выдвижения кредитором требований о досрочном исполнении договора. В связи с этим условия договоров, предписывающие уведомлять кредитора об изменении адреса регистрации (прописки), места работы, паспортных данных (замене паспорта), ущемляют права потребителя.

Аналогичные выводы содержатся и в иных судебных решениях (см., например, Решение Арбитражного суда Самарской области от 14.07.2017 по делу № А55-5923/2017).

Наличие ненадлежащим образом оформленных согласий

Оформление согласий субъектов ПДн на обработку и передачу данных третьим лицам часто сопряжено с нарушениями законодательства.

Так, распространенными видами нарушений финансовых организаций в данной области являются:

- включение в договор безальтернативных условий о согласии, вследствие чего оно не отвечает признаку конкретности;
- отсутствие разъяснений субъекту ПДн специальных терминов, содержащихся в согласии, вследствие чего оно не отвечает признаку информированности;

¹ Постановление Девятого арбитражного апелляционного суда от 09.10.2017 по делу № А40-26187/2017.

Контроль работы с персональными данными: нарушения и методы их предотвращения

— отсутствие уведомления субъекта ПДн о его праве на отзыв согласия;

— неполучение согласия на обработку ПДн третьих лиц (родственников заемщика или совместно с ним проживающих лиц) и обработка их ПДн не в соответствии с целью предоставления кредита.

Довольно частым нарушением является получение согласия субъекта ПДн в форме подписания договора кредитования с условием о согласии, вследствие чего согласие не получено свободно, волей и в интересе субъекта. В согласии указываются общие формулировки, которые позволяют оператору обрабатывать избыточные данные заемщиков, передавать данные заемщиков неопределенному кругу третьих лиц, а также обрабатывать ПДн родственников заемщика, не требуемые для целей предоставления кредита. Таким образом, в одном договоре кредитования может содержаться множество нарушений процедур сбора, обработки, хранения и передачи персональной информации.

Показательным является судебное дело, по итогам которого крупный банк был привлечен к административной ответственности по ч. 2 ст. 14.8 КоАП РФ на основании жалобы клиента в Роскомнадзор. Договор кредитования содержал пункт о даче потребителем согласия на предоставление банку врачебной информации о состоянии страхователя или застрахованного лица. Между тем включение такого пункта в анкету-заявление, выступающую неотъемлемой частью договора кредитования, нарушает требования к форме письменного согласия субъекта ПДн, а также нарушает режим врачебной тайны.

Суд в своем решении указал на то, что условие договора о необходимости разглашения сведений, составляющих врачебную тайну, ущемляет права потребителя. У страховщика появляется возможность получить от любого врача, больницы, поликлиники, другой организации или лица, владеющих любой информацией о страхователе/застрахованном, эту информацию, включая копии либо подлинники документов с указанием заболеваний или несчастных случаев, лечения, обследований и их результатов, консультаций или госпитализаций¹.

Страховая организация безуспешно пыталась обжаловать предписание Роскомнадзора, но в итоге также была привлечена к административной ответственности. В данном споре были выявлены нарушения как в части несоблюдения формы письменного согласия,

¹ Постановление Одиннадцатого арбитражного апелляционного суда от 08.09.2017 по делу № А-72-2343/2017.

Вячеслав ЧМЫХОВ Татьяна ДВЕНАДЦАТОВА

так и в части избыточной обработки, обработки данных третьих лиц и несоблюдения конфиденциальности ПДн.

Так, страховщик, ссылаясь на подписанный страхователем договор страхования, предусматривающий право застрахованного лица в любое время отозвать согласие, утверждал, что страхователь предоставил письменное согласие на обработку ПДн. Однако суд первой инстанции не принял этот довод.

По мнению суда, подписывая заранее разработанный текст договора страхования, напечатанный очень мелким шрифтом и содержащий такие специфические (используемые в целях Закона № 152-ФЗ и не используемые в обиходе) понятия и термины, как «обработка персональных данных», страхователь вряд ли был достаточно информирован об истинном смысле этих понятий и терминов, а также о возможных последствиях своего согласия. Содержащееся в договоре страхования согласие не является надлежащим, поскольку не отвечает требованиям о письменном согласии, изложенным в Законе № 152-ФЗ: согласие на обработку ПДн должно быть конкретным, информированным и сознательным и предполагать как минимум письменное разъяснение субъекту ПДн значения понятия «обработка персональных данных». Однако ни договор страхования, ни какой-либо другой документ не содержали никаких сведений о разъяснении страхователю указанного понятия.

Суд также отметил, что субъект ПДн принимает решение о предоставлении его ПДн и дает согласие на их обработку не просто путем подписания договора с условием о согласии, но выражая его свободно, своей волей и в своем интересе отдельно.

Более того, суд обратил внимание, что страховая организация, будучи оператором ПДн, получила право обрабатывать их в полном объеме, включая право на такие действия, как раскрытие неопределенному кругу лиц и передача на территорию иностранного государства, при этом необходимость подобных действий никак не обусловливается и не объясняется целями обработки. По мнению суда, данное обстоятельство свидетельствует об избыточности действий по обработке ПДн¹.

Дополнительной иллюстрацией нарушений, сопряженных с получением согласия субъекта ПДн, являются выводы, отраженные в Решении Арбитражного суда Уральского округа от 22.12.2016 по делу № А76-5164/2016. По результатам проверки банка социального развития был выявлен ряд нарушений, а именно: обработка ПДн

Договор кредитования содержал пункт о даче потребителем согласия на предоставление банку врачебной информации о состоянии страхователя или застрахованного лица. Это повлекло за собой привлечение банка к административной ответственности по ч. 2 ст. 14.8 КоАП РФ.

¹ Постановление Одиннадцатого арбитражного апелляционного суда от 17.07.2017 по делу № А65-4208/2017.

Контроль работы с персональными данными: нарушения и методы их предотвращения

членов семьи, проживающих совместно с клиентом; обработка ПДн совершеннолетних детей, проживающих отдельно от клиента; обработка ПДн родителей клиента. Все эти ПДн содержались в анкете-заявлении на предоставление кредита.

Суд в своем решении указал на то, что включение в анкету-заявление на предоставление кредита ПДн лиц, с которыми договор не заключается и которые не давали согласие на передачу и обработку своих ПДн, исключительно в целях расчета норматива банка, является прямым нарушением Закона № 152-ФЗ. Суд также отметил, что обязательность указания ПДн упомянутых лиц не зависит от того, имеются ли у них кредитные обязательства, которые могут повлиять на расчет норматива.

Регулирование внутренних процессов обработки персональных данных

При проверках контролирующие органы уделяют первоочередное внимание внутренним документам финансовых организаций, регулирующим процессы обработки ПДн.

Перечня обязательных к оформлению актов, регулирующих процессы обработки ПДн в компании, действующее законодательство не содержит. Таким образом, по причине пробела в регулировании организации зачастую задаются вопросом: какие локальные акты обязательны к оформлению, а какие являются опциональными?

Как правило, деятельность компании в части защиты ПДн регламентируют два базовых документа: Политика обработки персональных данных и Положение о защите, хранении, обработке и передаче персональных данных работников. К внутренней документации банков следует также отнести третий документ — Положение о защите, хранении, обработке и передаче персональных данных потребителей.

При составлении Политики обработки персональных данных (наличие которой в силу ст. 18.1 Закона № 152-ФЗ обязательно) финансовые организации могут смело руководствоваться рекомендациями Роскомнадзора¹, опубликованными в открытом доступе на официальном сайте ведомства.

Так, согласно рекомендациям Роскомнадзора в Политику обработки персональных данных необходимо включить следующие разделы:

Рекомендуем оформить отдельный регламент обработки персональных данных заемщиков и страхователей, в котором отразить все основные спорные вопросы, руководствуясь актуальной судебной практикой.

¹ Рекомендации по составлению документа, определяющего политику оператора в отношении обработки персональных данных, в порядке, установленном Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных».

Вячеслав ЧМЫХОВ Татьяна ДВЕНАДЦАТОВА

- общие положения;
- цели сбора и обработки;
- правовые основания обработки;
- объем и категории обрабатываемых данных;
- порядок и условия обработки;
- порядок реагирования на запросы субъектов в отношении обработки их данных;
- порядок модификации, удаления и блокировки данных.

Финансовым организациям также настоятельно рекомендуется оформить отдельный регламент обработки ПДн заемщиков и страхователей, в котором отразить все основные спорные вопросы, руководствуясь актуальной судебной практикой.

Также необходимо уделить особое внимание следующим внутренним документам:

- должностная инструкция ответственного за обработку ПДн в организации;
- перечень информационных систем, обрабатывающих ПДн в организации;
- матрица доступа в помещения, в которых расположены серверные мощности, обрабатывающие ПДн (как правило, содержат перечень лиц, имеющих такой доступ);
- матрица доступа в информационные системы, обрабатывающие ПДн (как правило, содержат перечень лиц, имеющих такой доступ);
- модель угроз безопасности ПДн при их обработке в информационных системах персональных данных.

Модель угроз представляется наиболее сложным для оформления локальным актом. Обязательность ее наличия обусловлена п. 5 ч. 1 ст. 18.1 Закона № 152-ФЗ. Для облегчения задачи рекомендуется при оформлении такого документа руководствоваться Стандартом Банка России СТО БР ИББС-1.0-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения».

Также не стоит забывать о наличии подписанных генеральным директором или другими уполномоченными лицами в соответствии с уставом приказов о назначении ответственных за обработку ПДн.

Выводы

Итак, что необходимо сделать в кредитной организации, исходя из анализа судебной практики и массива нарушений в области ПДн?

Контроль работы с персональными данными: нарушения и методы их предотвращения

1. В первую очередь — провести аудит процессов сбора и обработки ПДн и выявить потенциальные риски. Аудит поможет четко определить следующие «вводные»:

- круг и категории обрабатываемых ПДн;
- круг и категории субъектов, чьи данные обрабатываются;
- круг локальных актов, регулирующих процессы сбора и обработки ПДн;
- механизмы защиты и технические меры безопасности, обеспечивающие конфиденциальность данных и защищающих банк от утечки данных.

2. Следующий шаг — модифицировать и (или) внедрить внутреннюю документацию, регулирующую процессы сбора и обработки данных.

3. Пересмотреть типовые кредитные и страховые договоры, чтобы исключить из них пункты об обработке данных.

4. Составить типовые согласия на обработку данных, полностью соответствующие нормам действующего законодательства.

5. Обеспечить сбор данных, соответствующих целям такого сбора, исключив в перспективе избыточную обработку данных потребителей.

6. Обеспечить наличие письменных договоров с третьими лицами и партнерами, которым банк передает ПДн.

7. Дополнительно — составить политику взаимодействия с профильными государственными органами, включая Роскомнадзор. 