

**Политика обработки персональных данных
в Банке ВТБ (ПАО)**

2016

Содержание

1.	ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ	3
2.	ОБЩИЕ ПОЛОЖЕНИЯ	3
3.	ПРИНЦИПЫ ОБРАБОТКИ ПДН.....	3
4.	ЦЕЛИ ОБРАБОТКИ ПДН В БАНКЕ	3
5.	ОБЩИЙ ПОРЯДОК ОБРАБОТКИ ПДН	4
6.	ПРЕДОСТАВЛЕНИЕ ДОСТУПА К ПДН	7
7.	ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ОБРАБОТКИ ПДН	7
8.	ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ	8

1. Обозначения и сокращения

ИБ	Информационная безопасность.
ИСПДн	Информационная система персональных данных.
ПДн	Персональные данные.

2. Общие положения

2.1. Данная Политика обработки персональных данных в Банке ВТБ (ПАО) (далее – Политика) определяет основные принципы и правила обработки персональных данных в Банке ВТБ (ПАО) (далее – Банк) и является обязательной для выполнения всеми работниками Банка.

2.2. При необходимости положения данной Политики могут детализироваться и уточняться в отдельных нормативных и методических документах Банка.

2.3. Данная Политика разработана с учетом требований Федерального закона №152-ФЗ от 27 июля 2006 года «О персональных данных» и иных нормативных актов Российской Федерации, регулирующих порядок обработки и обеспечения информационной безопасности ПДн в организациях банковской системы Российской Федерации.

3. Принципы обработки ПДн

Основными принципами обработки ПДн в Банке являются:

- **законность:** любая деятельность в отношении ПДн осуществляется в соответствии с требованиями действующего законодательства Российской Федерации, руководящими документами, а также стандартами Центрального Банка Российской Федерации (как отраслевого регулятора);
- **целесообразность и целенаправленность:** ПДн в Банке обрабатываются в том и только в том объеме, который необходим для достижения заранее определенных целей обработки ПДн. В Банке обеспечивается соответствие порядка и способов обработки ПДн целям обработки ПДн. По достижении указанных целей обработка соответствующих ПДн прекращается;
- **безопасность:** все действия в отношении ПДн в Банке осуществляются таким образом, чтобы минимизировать возможность нанесения ущерба субъекту ПДн. Для этого в Банке реализуется комплекс мер, направленных на обеспечение ИБ сведений ограниченного распространения (защищаемой законом информации), к которым относятся ПДн, а также специальных мер и средств обеспечения ИБ ПДн.

4. Цели обработки ПДн в Банке

4.1. Целями обработки ПДн в Банке являются:

- осуществление возложенных на Банк законодательством Российской Федерации функций в соответствии с Налоговым кодексом Российской Федерации, федеральными законами, в частности: Федеральным законом от 02.12.1990 № 395-1 (ред. от 29.12.2015) «О банках и банковской деятельности», Федеральным законом от 30.12.2004 № 218-ФЗ (ред. от 30.12.2015) «О кредитных историях», Федеральным законом от 07.08.2001 № 115-ФЗ (ред. от 30.12.2015) «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», Федеральным законом от 10.12.2003 № 173-ФЗ (ред. от 30.12.2015) «О валютном регулировании и валютном контроле», Федеральным законом от 22.04.1996 № 39-ФЗ (ред. от 30.12.2015) «О рынке ценных бумаг», Федеральным законом от 26.10.2002 № 127-ФЗ (ред. от 29.12.2015) «О несостоятельности (банкротстве)», Федеральным законом от 01.04.1996 № 27-ФЗ (ред. от 01.12.2014) «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования», Федеральным законом от 27.07.2006 № 152-ФЗ (ред. от

21.07.2014) «О персональных данных», нормативными актами Банка России, а также Уставом и нормативными актами Банка;

- организация учета работников Банка для обеспечения соблюдения законов и иных нормативно-правовых актов, содействия в трудоустройстве, обучении, продвижении по работе, пользования различного вида льготами в соответствии с Трудовым кодексом Российской Федерации, Налоговым кодексом Российской Федерации, федеральными законами, в частности: Федеральным законом от 01.04.1996 № 27-ФЗ (ред. от 01.12.2014) «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования», Федеральным законом от 27.07.2006 № 152-ФЗ (ред. от 21.07.2014) «О персональных данных», а также Уставом и нормативными актами Банка.

4.2. Указанные выше цели обуславливают необходимость обработки ПДн работников и физических лиц - представителей клиентов Банка (юридических лиц) для выполнения следующих основных задач:

- заключения договоров с субъектами ПДн (их законными представителями) и их исполнения;
- обеспечения юридической значимости документов, образующихся в процессе исполнения договоров с клиентами, работниками, партнерами, контрагентами и прочими сторонними по отношению к Банку лицами и организациями;
- обеспечения возможности защиты имущественных и иных интересов Банка, его работников и клиентов;
- организации кадровой работы и учета работников Банка для содействия в трудоустройстве, обучении, продвижении по работе, пользования различного вида льготами;
- осуществления управленческой деятельности;
- контроля количества и качества предоставляемых Банком услуг;
- осуществления административно-хозяйственной деятельности;
- формирования отчетности, в том числе для предоставления регуляторам и государственным органам.

5. Общий порядок обработки ПДн

5.1. Обработка ПДн в Банке осуществляется только с согласия субъекта ПДн (его законного представителя¹ после проверки его полномочий) в случае, если получение такого согласия необходимо в соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ (ред. от 21.07.2014) «О персональных данных».

Формы письменного согласия на обработку ПДн устанавливаются нормативными и(или) методическими документами Банка, регламентирующими технологические и бизнес-процессы Банка, в рамках которых производится обработка ПДн.

Достоверность предоставляемых ПДн должна проверяться принимающим их работником путем их сверки с информацией, содержащейся в оригиналах документов или их надлежащим образом заверенных копиях, предъявляемых субъектом ПДн или его законным представителем.

5.2. Банк осуществляет передачу ПДн государственным органам и уполномоченным лицам² в рамках их полномочий и компетенции в соответствии с законодательством Российской

¹ В случае получения ПДн субъекта через его законного представителя, Банк уведомляет о данном факте субъекта ПДн и сообщает ему его права в отношении обрабатываемых ПДн, наименование и адрес Банка, цели обработки ПДн, предполагаемых пользователей ПДн. Исключение составляют случаи, когда:

- ПДн переданы в Банк на основании требований федерального закона;
- ПДн являются общедоступными;
- Банк осуществляет обработку ПДн по поручению третьего лица – оператора на основании договора, заключенного между Банком и таким третьим лицом.

² Представителю субъекта ПДн (в том числе адвокату) ПДн передаются в порядке, регламентированном действующим законодательством Российской Федерации и объеме, установленном распоряжением субъекта ПДн, при наличии одного из следующих надлежащим образом оформленных документов:

- оригинала нотариально удостоверенной доверенности представителя субъекта ПДн;

Федерации. Процедуры передачи ПДн и их носителей, а также их учета выполняются в соответствии с установленным в Банке порядком ведения делопроизводства и соответствующими нормативными документами Банка.

5.3. Банк может осуществлять передачу ПДн для обработки третьему лицу, если иное не предусмотрено законодательством Российской Федерации. При этом:

- обработка третьим лицом ПДн, предоставленных Банку субъектом ПДн (его законным представителем), может осуществляться только с согласия субъекта ПДн (его законного представителя), если получение такого согласия необходимо в соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ (ред. от 21.07.2014) «О персональных данных»;
- обработка ПДн третьим лицом может осуществляться только на основании договора, в котором определены перечень действий (операций), которые будут осуществляться с ПДн, а также положения по обеспечению ИБ ПДн, в том числе требования не раскрывать и не распространять ПДн без согласия субъекта ПДн, если иное не предусмотрено законодательством Российской Федерации.

Процедуры передачи ПДн и их носителей, а также их учета выполняются в соответствии с установленным в Банке порядком ведения делопроизводства и соответствующими нормативными документами Банка.

5.4. Банк может осуществлять трансграничную передачу ПДн в случаях, предусмотренных законодательством Российской Федерации, договорами и соглашениями с международными организациями. При этом в указанные договоры и соглашения должны быть включены положения по обеспечению адекватной защиты прав субъектов ПДн (в том числе положения по обеспечению ИБ ПДн).

5.5. Банк обрабатывает ПДн работников и физических лиц - представителей клиентов Банка (юридических лиц), и при этом не обрабатывает специальных категорий ПДн, касающихся расовой и национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни, судимости физических лиц.

5.6. Банк осуществляет деятельность по своевременному выявлению и внесению изменений в обрабатываемые ПДн с целью обеспечения их точности, достоверности и актуальности, в том числе по отношению к целям обработки ПДн. Соответствующие процедуры и инструкции устанавливаются нормативными и(или) методическими документами Банка, регламентирующими технологические и бизнес-процессы Банка, в рамках которых производится обработка ПДн.

Изменения в ПДн вносятся уполномоченным работником Банка только на основании предоставленных надлежащим образом оформленных оригиналов документов или их заверенных копий.

В случае выявления неточных ПДн субъектом ПДн и при обращении субъекта ПДн или его законного представителя, либо по их запросу или по запросу уполномоченного органа по защите прав субъектов ПДн Банк обеспечивает их блокирование с момента такого обращения или получения указанного запроса на период проверки, если блокирование ПДн не нарушает права и законные интересы субъекта ПДн или третьих лиц.

В случае подтверждения факта неточности ПДн на основании сведений, предоставленных субъектом ПДн или его представителем либо уполномоченным органом по защите прав субъектов ПДн, или иных необходимых документов, Банк обеспечивает их уточнение в установленный срок со дня предоставления таких сведений и снимает их блокирование.

В случае, если факт неточности ПДн не подтверждается на основании сведений, предоставленных субъектом ПДн или его представителем либо уполномоченным органом по защите прав субъектов ПДн, или иных необходимых документов, Банк снимает их блокирование.

5.7. Хранение ПДн в форме, позволяющей идентифицировать субъекта ПДн, осуществляется не дольше, чем того требует достижение целей их обработки, если иное не

- заявления субъекта ПДн, написанного в присутствии работника Банка и заверенного работником Банка, принявшим заявление (или заверенного нотариально, если оно составлялось не в присутствии работника Банка). В случае если лицо, обратившееся в Банк с запросом на предоставление ПДн, не уполномочено на получение информации, относящейся к ПДн, Банк обязан отказать лицу в выдаче такой информации с соответствующим уведомлением указанного лица об отказе.

установлено законодательством Российской Федерации или договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн.

Обрабатываемые ПДн подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено законодательством Российской Федерации. Процедуры уничтожения и обезличивания ПДн устанавливаются методическими документами Банка, регламентирующими аналогичные процедуры в отношении сведений ограниченного распространения, к которым относятся ПДн, и их носителей.

5.8. Хранение ПДн при обработке с использованием средств автоматизации осуществляется обособленно от иной информации, в частности путем фиксации на отдельных материальных носителях (при наличии технической возможности), а при обработке ПДн на бумажных носителях – в специальных разделах или в полях форм документов³.

При фиксации ПДн на материальных носителях не допускается фиксация на одном материальном носителе ПДн, цели обработки которых заведомо не совместимы. Для обработки различных категорий ПДн, осуществляемой без использования средств автоматизации, для каждой категории ПДн используется отдельный материальный носитель.

5.9. По достижении целей обработки ПДн или по требованию субъекта ПДн (его законного представителя) ПДн уничтожаются или обезличиваются, если иное не установлено законодательством Российской Федерации.

В случае выявления неправомерной обработки ПДн при обращении субъекта ПДн или его законного представителя, по запросу субъекта ПДн / его представителя или уполномоченного органа по защите прав субъектов ПДн Банк обеспечивает блокирование неправомерно обрабатываемых ПДн, относящихся к этому субъекту ПДн, с момента такого обращения или получения указанного запроса на период проверки и инициирует служебное расследование в установленном в Банке порядке.

В случае если обеспечить правомерность обработки ПДн невозможно, Банк в установленный срок с даты выявления неправомерной обработки ПДн, обеспечивает уничтожение таких ПДн. Об устранении допущенных нарушений или об уничтожении ПДн Банк сообщает субъекту ПДн или его законному представителю, а в случае если обращение субъекта ПДн или его законного представителя либо запрос уполномоченного органа по защите прав субъектов ПДн были направлены уполномоченным органом по защите прав субъектов ПДн, также указанный орган.

В случае достижения цели обработки ПДн Банк прекращает обработку ПДн, проводит анализ факта достижения цели обработки ПДн и в случае положительного результата обеспечивает уничтожение соответствующих ПДн в установленный срок с даты достижения цели обработки ПДн, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, иным соглашением между Банком и субъектом ПДн либо если Банк не вправе осуществлять обработку ПДн без согласия субъекта ПДн на основаниях, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ (ред. от 21.07.2014) «О персональных данных» или другими федеральными законами.

В случае отсутствия возможности уничтожения ПДн в течение срока, установленного законодательством Российской Федерации, Банк обеспечивает блокирование таких ПДн с последующим обеспечением уничтожения ПДн, которое производится не позднее 6 (шести) месяцев со дня их блокирования.

³ Типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должна:

- содержать сведения о цели обработки ПДн, осуществляемой без использования средств автоматизации; наименование и адрес подразделения Банка, обрабатывающего ПДн; фамилию, имя, отчество и адрес субъекта ПДн; источник получения ПДн; сроки обработки ПДн; перечень действий с ПДн, которые будут совершаться в процессе их обработки; общее описание используемых оператором способов обработки ПДн.
- предусматривать поле или приложение, в котором субъект ПДн может поставить отметку о своем согласии на обработку ПДн, при необходимости получения письменного согласия на обработку ПДн;
- быть составлена таким образом, чтобы каждый из субъектов ПДн, содержащихся в документе, имел возможность ознакомиться со своими ПДн, содержащимися в документе, не нарушая прав и законных интересов иных субъектов ПДн;
- исключать объединение полей, предназначенных для внесения ПДн, цели обработки которых заведомо не совместимы.

Уничтожение части ПДн, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих ПДн с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

5.10. Ответственность за организацию процесса обработки ПДн возлагается на работника Банка приказом по Банку.

5.11. В область его ответственности входит:

- контроль выполнения требований по обеспечению ИБ ПДн, в том числе при обработке их в информационных системах персональных данных (ИСПДн);
- организация контроля прекращения обработки и обезличивания или уничтожения ПДн;
- организация процесса обработки запросов субъектов ПДн (их законных представителей) и уполномоченного органа по защите прав субъектов ПДн;
- формирование и направление уведомлений уполномоченному органу по защите прав субъектов ПДн об обработке ПДн в сроки, установленные законодательством Российской Федерации.

Для исполнения обязанностей по обеспечению ИБ ПДн данное лицо имеет право:

- принимать решения в пределах своей компетенции;
- требовать от работников Банка соблюдения действующего законодательства, а также локальных нормативных актов Банка, содержащих требования по защите ПДн;
- контролировать осуществление мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ (ред. от 21.07.2014) «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами.

5.12. Банк осуществляет уведомление уполномоченного органа по защите прав субъектов ПДн об обработке ПДн в сроки, установленные Федеральным законом от 27.07.2006 № 152-ФЗ (ред. от 21.07.2014) «О персональных данных».

6. Предоставление доступа к ПДн

6.1. Доступ к ПДн предоставляется только тем работникам Банка, которым он необходим для выполнения их функциональных и должностных обязанностей.

6.2. В Банке ведется учет работников, имеющих доступ к ПДн.

6.3. Работники Банка, имеющие доступ к ПДн, обязаны знать и выполнять требования законодательства Российской Федерации в области обработки и обеспечения ИБ ПДн, а также требования настоящей Политики и нормативных документов Банка, детализирующих ее положения.

6.4. Указанные работники проходят соответствующий инструктаж при приеме на работу и(или) при получении ролей, предусматривающих наличие/расширение доступа к ПДн. Уполномоченный работник Банка, проводящий инструктаж, информирует лицо, допущенное к обработке ПДн, о факте обработки им ПДн, категориях обрабатываемых ПДн, а также об особенностях и правилах осуществления такой обработки (включая ознакомление с нормативно-методическими документами под роспись).

6.5. Передача ПДн внутри Банка может осуществляться только между работниками, имеющими доступ к ПДн.

6.6. Право субъекта ПДн на доступ к его ПДн может быть ограничено в соответствии с законодательством Российской Федерации, в том числе в случае если обработка ПДн осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма.

7. Обеспечение безопасности обработки ПДн

7.1. В Банке определены угрозы ИБ и реализован комплекс организационно-технических мер в отношении сведений ограниченного распространения (защищаемой законом

информации), к которым относятся ПДн, а также специальных мер и средств обеспечения ИБ ПДн, направленных на предотвращение несанкционированного или случайного доступа к ПДн, их уничтожения, искажения, блокирования, распространения и иных неправомерных действий.

7.2. К мерам обеспечения ИБ ПДн в Банке относятся в том числе:

- учет ПДн и их носителей;
- учет и классификация ИСПДн;
- формализация и контроль выполнения порядка обработки ПДн в ИСПДн;
- формализация и контроль выполнения требований по уничтожению (обезличиванию) ПДн и носителей ПДн;
- контроль доступа работников Банка и иных лиц к обрабатываемым в Банке ПДн и средствам их обработки;
- контроль соблюдения работниками Банка, осуществляющими обработку ПДн, правил, требований и процедур обработки ПДн;
- раздельное хранение ПДн, обработка которых осуществляется с различными целями;
- включение положений по обеспечению ИБ ПДн в договоры с третьими лицами, которым передаются ПДн, в том числе требований не раскрывать и не распространять ПДн без согласия субъекта ПДн, если иное не предусмотрено законодательством Российской Федерации.

7.3. Определение, фиксация и выполнение требований по обеспечению ИБ ПДн выполняется в том же порядке, что и определение, фиксация и выполнение требований по обеспечению ИБ иных сведений ограниченного распространения (охраняемой законом информации) в Банке.

8. Заключительные положения

8.1. Ответственность за разглашение или утрату ПДн, обрабатываемых в Банке, несет персонально каждый работник Банка, имеющий доступ к этим ПДн и допустивший их разглашение или утрату.

8.2. По факту разглашения или утраты ПДн в Банке проводится служебное расследование в установленном порядке.

8.3. Одновременно с проведением служебного расследования в Банке принимаются меры по минимизации нежелательных последствий произошедшего, а также по недопущению (предотвращению) в дальнейшем разглашения или утраты ПДн.

8.4. Ответственность за контроль над соблюдением настоящей Политики возлагается на лицо, назначенное приказом Банка ответственным за организацию процесса обработки ПДн в Банке.

8.5. Политика обеспечения ИБ ПДн публикуется на сайте Банка в открытом доступе.

8.6. Данная Политика пересматривается и актуализируется при изменении законодательства Российской Федерации, регулирующего права и обязанности Банка в области обработки и обеспечения ИБ ПДн и(или) изменения соответствующих обязательств Банка, но не реже, чем раз в 3 года.