УТВЕРЖДЕНО:
Правлением ПАО «Донкомбанк»
Протокол № 24
от « _28_ » ____02____ 2023 г.

Положение
об обработке персональных данных ПАО «Донкомбанк»

г. Ростов-на-Дону

2023 г.

Содержание:

1. Общие положения

Целью настоящего Положения является обеспечение защиты персональных данных (далее - ПДн) при их обработке в ПАО «Донкомбанк» (далее - Банк).

Настоящее Положение разработано в соответствии с Конституцией РФ от 12.12.1993, Гражданским кодексом РФ от 26.01.1996 № 14-ФЗ, Трудовым Кодексом от 30.12.2001 № 197-ФЗ, федеральными законами от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 02.12.1990 № 395-1 «О банках и банковской деятельности», от 27.07.2006 № 152-ФЗ «О персональных данных» (далее - Федеральный закон), Постановлением Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» (далее – Постановление Правительства РФ № 1119), Приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер» (далее - ГОСТ Р 57580.1-2017) и иными нормативно-правовыми актами, действующими на территории Российской Федерации.

В настоящем Положении используются следующие основные понятия:

1) персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

1.1) персональные данные, разрешенные субъектом персональных данных для распространения, - персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном Федеральным законом;

2) оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными (Банк является оператором);

3) обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

4) автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники;

5) распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

6) предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

7) блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

8) уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

9) обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

10) информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

11) трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

Приказом Банка назначается ответственный за организацию обработки ПДн.

Все работники Банка, должностными инструкциями которых предусмотрена обработка ПДн, ознакамливаются с Федеральным законом и настоящим Положением под подпись при приеме на работу.

Банк в соответствии с требованиями статьи 22 Федерального закона уведомляет уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку ПДн, а также изменениях условий обработки ПДн.

Настоящее положение подлежит официальному опубликованию в информационно-телекоммуникационной сети «Интернет» на официальном сайте Банка.

2. Сведения, составляющие ПДн

Сведениями, составляющими ПДн, в Банке является любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту ПДн), в том числе:

1. Фамилия, имя, отчество (в т.ч. прежние), дата и место рождения.
2. Паспортные данные или данные иного документа, удостоверяющего личность (серия, номер, дата выдачи, наименование органа, выдавшего документ) и гражданство.
3. Характеристики, идентифицирующие физиологические особенности человека и на основе которых можно установить его личность.
4. Адрес места жительства (по паспорту и фактический) и дата регистрации по месту жительства или по месту пребывания.
5. Номера телефонов (мобильного и домашнего), в случае их регистрации на субъекта персональных данных или по адресу его места жительства (по паспорту).
6. Сведения об образовании, квалификации и о наличии специальных знаний или специальной подготовки (серия, номер, дата выдачи диплома, свидетельства, аттестата или другого документа об окончании образовательного учреждения, наименование и местоположение образовательного учреждения, дата начала и завершения обучения, факультет или отделение, квалификация и специальность по окончании образовательного учреждения, ученая степень, ученое звание, владение иностранными языками и другие сведения).
7. Сведения о повышении квалификации и переподготовке (серия, номер, дата выдачи документа о повышении квалификации или о переподготовке, наименование и местоположение образовательного учреждения, дата начала и завершения обучения, квалификация и специальность по окончании образовательного учреждения и другие сведения).
8. Сведения о трудовой деятельности (данные о трудовой занятости на текущее время с полным указанием должности, подразделения, наименования, адреса и телефона организации, а также реквизитов других организаций с полным наименование

занимаемых ранее в них должностей и времени работы в этих организациях, а также другие сведения).

9. Сведения о номере, серии и дате выдачи трудовой книжки (вкладыша в нее) и записях в ней.

10. Содержание и реквизиты трудового договора с работником Банка или гражданско-правового договора с гражданином.

11. Сведения о заработной плате (номера счетов для расчета с работниками, данные зарплатных договоров с клиентами, в том числе номера их спецкартсчетов, данные по окладу, надбавкам, налогам и другие сведения).

12. Сведения о воинском учете военнообязанных лиц и лиц, подлежащих призыву на военную службу (серия, номер, дата выдачи, наименование органа, выдавшего военный билет, военно-учетная специальность, воинское звание, данные о принятии\снятии на(с) учет(а) и другие сведения).

13. Сведения о семейном положении (состояние в браке, данные свидетельства о заключении брака, фамилия, имя, отчество супруга(и), паспортные данные супруга(и), данные брачного контракта, данные справки по форме 2-НДФЛ супруга(и), данные документов по долговым обязательствам, степень родства, фамилии, имена, отчества и даты рождения других членов семьи, иждивенцев и другие сведения).

14. Сведения об имуществе (имущественном положении):

- автотранспорт (государственные номера и другие данные из свидетельств о регистрации транспортных средств и из паспортов транспортных средств);
- недвижимое имущество (вид, тип, способ получения, общие характеристики, стоимость, полные адреса размещения объектов недвижимости и другие сведения);
- банковские вклады (данные договоров с клиентами, в том числе номера их счетов, спецкартсчетов, вид, срок размещения, сумма, условия вклада и другие сведения);
- кредиты (займы), банковские счета (в том числе спецкартсчета), денежные средства и ценные бумаги, в том числе в доверительном управлении и на доверительном хранении (данные договоров с клиентами, в том числе номера счетов, спецкартсчетов, номера банковских карт, кодовая информация по банковским картам, коды кредитных историй, адреса приобретаемых объектов недвижимости, сумма и валюта кредита или займа, цель кредитования, условия кредитования, сведения о залоге, сведения о приобретаемом объекте, данные по ценным бумагам, остатки и суммы движения по счетам, тип банковских карт, лимиты и другие сведения).

15. Сведения о номере и серии страхового свидетельства государственного пенсионного страхования.

16. Сведения об идентификационном номере налогоплательщика.

17. Сведения из страховых полисов обязательного (добровольного) медицинского страхования (в том числе данные соответствующих карточек медицинского страхования).

18. Сведения, указанные в оригиналах и копиях приказов по личному составу Банка и материалах к ним.

19. Сведения о государственных и ведомственных наградах, почетных и специальных званиях, поощрениях (в том числе наименование или название награды, звания или поощрения, дата и вид нормативного акта о награждении или дата поощрения) работников Банка.

20. Материалы по аттестации и оценке работников Банка.

21. Материалы по внутренним служебным расследованиям в отношении работников Банка.

22. Внутрибанковские материалы по расследованию и учету несчастных случаев на производстве и профессиональным заболеваниям в соответствии с Трудовым кодексом Российской Федерации, другими федеральными законами.

23. Сведения о временной нетрудоспособности работников Банка.

24. Табельный номер работника Банка.

25. Сведения о социальных льготах и о социальном статусе (серия, номер, дата выдачи, наименование органа, выдавшего документ, являющийся основанием для предоставления льгот и статуса, и другие сведения).

26. Сведения о должнике, просроченной задолженности и ее взыскании и любые другие персональные данные должника.

Выделяются следующие категории ПДн:

- специальные категории ПДн (сведения, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни);
- биометрические ПДн (сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных);
- ПДн, полученные из общедоступных источников, созданных в соответствии со статьей 8 Федерального закона;
- иные ПДн (ПДн, которые не могут быть отнесены к специальным категориям ПДн, к биометрическим категориям ПДн, к ПДн, полученным из общедоступных источников).

3. Цели обработки персональных данных

Целью обработки ПДн в Банке является:

- осуществление возложенных на Банк законодательством Российской Федерации функций в соответствии с Налоговым кодексом Российской Федерации, федеральными законами, в частности: «О банках и банковской деятельности», «О кредитных историях», «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», «О валютном регулировании и валютном контроле», «О рынке ценных бумаг», «О несостоятельности (банкротстве) кредитных организаций», «О страховании вкладов физических лиц в банках Российской Федерации», «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования», «О персональных данных», нормативными актами Банка России, а также Уставом и нормативными актами Банка;

- организация учета сотрудников кредитной организации для обеспечения соблюдения законов и иных нормативно-правовых актов, содействия сотруднику в трудоустройстве, обучении, служебном продвижении, пользования различного вида льготами в соответствии с Трудовым кодексом Российской Федерации, Налоговым кодексом Российской Федерации, федеральными законами, в частности: «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования», «О персональных данных», а также Уставом и нормативными актами Банка.

4. Объем и содержание ПДн

Объем и содержание ПДн, обрабатываемых Банком, а также перечень действий и способы обработки, определяются, исходя из целей обработки, и фиксируются во внутренних положениях, регламентах, инструкциях Банка.

5. Сроки обработки ПДн

Сроки обработки, указанных выше ПДн, определяются в соответствие со сроком действия договора с субъектом ПДн, Приказом Росархива от 20.12.2019 № 236 «Об утверждении Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков их хранения», Постановлением ФКЦБ РФ от 16.07.2003

№ 03-33/пс «Об утверждении Положения о порядке и сроках хранения документов акционерных обществ», сроком исковой давности, а также иными требованиями законодательства и нормативными документами Банка России.

6. Информационные системы персональных данных (ИСПДн) Банка

В информационной системе Банка функционирует несколько автоматизированных систем (далее - АС) и прикладных программ, реализующих информационный и платежный банковские технологические процессы, в рамках которых обрабатываются ПДн.

При обработке ПДн в ИСПДн Банка соблюдаются требования, установленные Постановлением Правительства РФ № 1119.

При обработке ПДн в АС устанавливаются четыре уровня защищенности ПДн.

Уровень защищенности АС Банка определяется в соответствии с актуальными угрозами для каждой ИСПДн.

В соответствии с комплексом документов в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации», угрозы утечки ПДн по техническим каналам, а также угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в ИСПДн, признаются неактуальными для Банка.

Перечень ИСПДн утверждается председателем правления Банка.

Для ресурсов ПДн, обрабатываемых в ИСПДн Банка, порядок обработки ПДн определяется в соответствии с эксплуатационной документации на АС, разрабатываемой на этапе создания или модернизации АС и внутренними положениями (инструкциями, регламентами).

7. Доступ к ПДн

Сотрудники Банка имеют доступ к ПДн только в рамках своих служебных обязанностей и для их выполнения, соблюдая необходимые организационные и технические меры защиты ПДн. Доступ к ПДн осуществляется с учетом «Перечня должностей работников ПАО «Донкомбанк», предусматривающих доступ к персональным данным», который утверждается Председателем правления Банка.

Доступ сотрудников Банка к ИСПДн осуществляется в соответствии с «Положением об организации доступа и разграничении полномочий при работе с информационной системой ПАО «Донкомбанк».

Сотрудники Банка получают доступ к обработке ПДн только после ознакомления под роспись с настоящим Положением и «Инструкцией пользователя при обработке персональных данных в информационной системе ПАО «Донкомбанк», приведенной в приложении 1 настоящего Положения.

В Банке определен и документально зафиксирован порядок доступа работников и иных лиц в помещения, в которых ведется обработка ПДн. Правила доступа в помещения, где ведется обработка ПДн, приведены в приложении 2 настоящего Положения.

Перечень помещений ПАО «Донкомбанк», в которых осуществляется обработка персональных данных, утверждается приказом Банка.

8. Сбор и обработка персональных данных

Обработка ПДн субъекта должна осуществляться исключительно для обеспечения соблюдения законов и иных нормативных правовых актов, предусмотренных законодательством РФ и актами Банка, а также осуществления основной деятельности Банка. Обработка ПДн осуществляется с соблюдением принципов и правил, предусмотренных законодательством.

Все ПДн о субъекте Банк может получить у него самого или у лица, не являющегося субъектом ПДн, при условии предоставления Банку подтверждения наличия оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона. Субъект обязан предоставлять Банку достоверные сведения о себе и своевременно сообщать ему об изменении своих ПДн.

В соответствии с Федеральным законом, обработка ПДн допускается в следующих случаях:

1) обработка ПДн осуществляется с согласия субъекта ПДн на обработку его ПДн;

2) обработка ПДн необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на Банк функций, полномочий и обязанностей;

3) обработка ПДн осуществляется в связи с участием лица в конституционном, гражданском, административном, уголовном судопроизводстве, судопроизводстве в арбитражных судах;

3.1) обработка ПДн необходима для исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве (далее - исполнение судебного акта);

4) обработка ПДн необходима для исполнения полномочий федеральных органов исполнительной власти, органов государственных внебюджетных фондов, исполнительных органов государственной власти субъектов Российской Федерации, органов местного самоуправления и функций организаций, участвующих в предоставлении соответственно государственных и муниципальных услуг, предусмотренных Федеральным законом от 27 июля 2010 года № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», включая регистрацию субъекта персональных данных на едином портале государственных и муниципальных услуг и (или) региональных порталах государственных и муниципальных услуг;

5) обработка ПДн необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн, в том числе в случае реализации Банком своего права на уступку прав (требований) по такому договору, а также для заключения договора по инициативе субъекта ПДн или договора, по которому субъект ПДн будет являться выгодоприобретателем или поручителем. Заключаемый с субъектом ПДн договор не может содержать положения, ограничивающие права и свободы субъекта ПДн, устанавливающие случаи обработки ПДн несовершеннолетних, если иное не предусмотрено законодательством Российской Федерации, а также положения, допускающие в качестве условия заключения договора бездействие субъекта ПДн;

6) обработка ПДн необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта ПДн, если получение согласия субъекта ПДн невозможно;

7) обработка ПДн необходима для осуществления прав и законных интересов Банка или третьих лиц, в том числе в случаях, предусмотренных Федеральным законом «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», либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта ПДн;

8) обработка ПДн необходима для осуществления профессиональной деятельности журналиста и (или) законной деятельности средства массовой информации либо научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и законные интересы субъекта ПДн;

9) обработка ПДн осуществляется в статистических или иных исследовательских целях, за исключением целей, указанных в статье 15 Федерального закона, при условии обязательного обезличивания ПДн;

10) обработка ПДн, полученных в результате обезличивания персональных данных, осуществляется в целях повышения эффективности государственного или муниципального управления, а также в иных целях, предусмотренных Федеральным законом от 24 апреля 2020 года № 123-ФЗ «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации - городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных» и Федеральным законом от 31 июля 2020 года № 258-ФЗ «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации», в порядке и на условиях, которые предусмотрены указанными Федеральными законами;

11) осуществляется обработка ПДн, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

Банк вправе поручить обработку ПДн другому лицу с согласия субъекта ПДн, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия государственным органом или муниципальным органом соответствующего акта (далее - поручение Банка). Лицо, осуществляющее обработку ПДн по поручению Банка, обязано соблюдать принципы и правила обработки ПДн, предусмотренные Федеральным законом, соблюдать конфиденциальность ПДн, принимать необходимые меры, направленные на обеспечение выполнения обязанностей, предусмотренных Федеральным законом. В поручении Банка должны быть определены перечень ПДн, перечень действий (операций) с ПДн, которые будут совершаться лицом, осуществляющим обработку ПДн, цели их обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность ПДн, требования, предусмотренные частью 5 статьи 18 и статьей 18.1 Федерального закона, обязанность по запросу Банка в течение срока действия поручения Банка, в том числе до обработки ПДн, предоставлять документы и иную информацию, подтверждающие принятие мер и соблюдение в целях исполнения поручения Банка требований, установленных в соответствии с настоящим пунктом, обязанность обеспечивать безопасность ПДн при их обработке, а также должны быть указаны требования к защите обрабатываемых ПДн в соответствии со статьей 19 Федерального закона, в том числе требование об уведомлении Банка о случаях, предусмотренных частью 3.1 статьи 21 Федерального закона.

Лицо, осуществляющее обработку ПДн по поручению Банка, не обязано получать согласие субъекта ПДн на обработку его ПДн.

8.1. Обработка специальных категорий ПДн, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, не допускается, за исключением следующих случаев:

1) субъект ПДн дал согласие в письменной форме на обработку своих ПДн;

2) обработка ПДн, разрешенных субъектом персональных данных для распространения, осуществляется с соблюдением запретов и условий, предусмотренных статьей 10.1 Федерального закона;

2.1) обработка персональных данных необходима в связи с реализацией международных договоров Российской Федерации о реадмиссии;

2.2) обработка ПДн осуществляется в соответствии с Федеральным законом от 25 января 2002 года № 8-ФЗ «О Всероссийской переписи населения»;

2.3) обработка ПДн осуществляется в соответствии с законодательством о государственной социальной помощи, трудовым законодательством, пенсионным законодательством Российской Федерации;

3) обработка ПДн необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта ПДн либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия субъекта ПДн невозможно;

4) обработка ПДн осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка ПДн осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну;

5) обработка ПДн членов (участников) общественного объединения или религиозной организации осуществляется соответствующими общественным объединением или религиозной организацией, действующими в соответствии с законодательством Российской Федерации, для достижения законных целей, предусмотренных их учредительными документами, при условии, что ПДн не будут распространяться без согласия в письменной форме субъектов ПДн;

6) обработка ПДн необходима для установления или осуществления прав субъекта ПДн или третьих лиц, а равно и в связи с осуществлением правосудия;

7) обработка ПДн осуществляется в соответствии с законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-розыскной деятельности, об исполнительном производстве, уголовно-исполнительным законодательством Российской Федерации;

7.1) обработка полученных в установленных законодательством Российской Федерации случаях ПДн осуществляется органами прокуратуры в связи с осуществлением ими прокурорского надзора;

8) обработка ПДн осуществляется в соответствии с законодательством об обязательных видах страхования, со страховым законодательством;

9) обработка ПДн осуществляется в случаях, предусмотренных законодательством Российской Федерации, государственными органами, муниципальными органами или организациями в целях устройства детей, оставшихся без попечения родителей, на воспитание в семьи граждан;

10) обработка ПДн осуществляется в соответствии с законодательством Российской Федерации о гражданстве Российской Федерации.

Обработка ПДн, касающихся состояния здоровья, полученных в результате обезличивания персональных данных, допускается в целях повышения эффективности государственного или муниципального управления, а также в иных целях, предусмотренных Федеральным законом от 24 апреля 2020 года № 123-ФЗ «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации - городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных» и Федеральным законом от 31 июля 2020 года № 258-ФЗ «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации», в порядке и на условиях, которые предусмотрены указанными Федеральными законами.

Обработка ПДн объектов государственной охраны и членов их семей осуществляется с учетом особенностей, предусмотренных Федеральным законом от 27 мая 1996 года № 57-ФЗ «О государственной охране».

Обработка ПДн о судимости может осуществляться государственными органами или муниципальными органами в пределах полномочий, предоставленных им в

соответствии с законодательством Российской Федерации, а также иными лицами в случаях и в порядке, которые определяются в соответствии с федеральными законами.

Обработка специальных категорий ПДн должна быть незамедлительно прекращена, если устранены причины, вследствие которых осуществлялась обработка, если иное не установлено федеральным законом.

8.2. Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические ПДн) и которые используются Банком для установления личности субъекта ПДн, могут обрабатываться только при наличии согласия в письменной форме субъекта ПДн.

Обработка биометрических ПДн может осуществляться без согласия субъекта ПДн в связи с реализацией международных договоров Российской Федерации о реадмиссии, в связи с осуществлением правосудия и исполнением судебных актов, в связи с проведением обязательной государственной дактилоскопической регистрации, а также в случаях, предусмотренных законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-розыскной деятельности, о государственной службе, уголовно-исполнительным законодательством Российской Федерации, законодательством Российской Федерации о порядке выезда из Российской Федерации и въезда в Российскую Федерацию, о гражданстве Российской Федерации, законодательством Российской Федерации о нотариате.

Предоставление биометрических ПДн не может быть обязательным, за исключением случаев, предусмотренных абзацем 2 настоящего подпункта. Банк не вправе отказывать в обслуживании в случае отказа субъекта ПДн предоставить биометрические ПДн и (или) дать согласие на обработку ПДн, если в соответствии с федеральным законом получение Банком согласия на обработку ПДн не является обязательным.

9. Согласие на обработку ПДн

Субъект ПДн принимает решение о предоставлении его ПДн и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку ПДн должно быть конкретным, предметным, информированным, сознательным и однозначным. Согласие на обработку ПДн может быть дано субъектом ПДн или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом. В случае получения согласия на обработку ПДн от представителя субъекта ПДн полномочия данного представителя на дачу согласия от имени субъекта ПДн проверяются Банком.

Согласие на обработку ПДн может быть отозвано субъектом ПДн. В случае отзыва субъектом ПДн согласия на обработку ПДн Банк вправе продолжить обработку ПДн без согласия субъекта ПДн при наличии оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона.

Обязанность предоставить доказательство получения согласия субъекта ПДн на обработку его ПДн или доказательство наличия оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона, возлагается на Банк.

В случаях, предусмотренных Федеральным законом, обработка ПДн осуществляется только с согласия в письменной форме субъекта ПДн. Равнозначным содержащему собственноручную подпись субъекта ПДн согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью.

Согласие в письменной форме субъекта ПДн на обработку его ПДн должно включать в себя, в частности:

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

2) фамилию, имя, отчество, адрес представителя субъекта ПДн, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта ПДн);

3) наименование или фамилию, имя, отчество и адрес Банка, получающего согласие субъекта ПДн;

4) цель обработки ПДн;

5) перечень ПДн, на обработку которых дается согласие субъекта ПДн;

6) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению Банка, если обработка будет поручена такому лицу;

7) перечень действий с ПДн, на совершение которых дается согласие, общее описание используемых Банком способов обработки ПДн;

8) срок, в течение которого действует согласие субъекта ПДн, а также способ его отзыва, если иное не установлено федеральным законом;

9) подпись субъекта ПДн.

В случае недееспособности субъекта ПДн согласие на обработку его ПДн дает законный представитель субъекта ПДн.

В случае смерти субъекта ПДн согласие на обработку его ПДн дают наследники субъекта ПДн, если такое согласие не было дано субъектом ПДн при его жизни.

Типовая форма согласия субъектов ПДн на обработку их ПДн приведена в приложении 3 настоящего Положения.

Правила обработки и хранения в письменной форме согласий на обработку ПДн устанавливаются внутренними положениями (инструкциями, регламентами).

10. Общедоступные источники ПДн

В целях информационного обеспечения могут создаваться общедоступные источники ПДн (в том числе справочники). В общедоступные источники ПДн с письменного согласия субъекта ПДн могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные ПДн, сообщаемые субъектом ПДн.

Сведения о субъекте Пдн должны быть в любое время исключены из общедоступных источников ПДн по требованию субъекта ПДн либо по решению суда или иных уполномоченных государственных органов.

11. Трансграничная передача

Трансграничная передача персональных данных осуществляется в соответствии с Федеральным законом и международными договорами Российской Федерации.

Банк до начала осуществления деятельности по трансграничной передаче персональных данных обязан уведомить уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять трансграничную передачу персональных данных. Указанное уведомление направляется отдельно от уведомления о намерении осуществлять обработку персональных данных, предусмотренного статьей 22 Федерального закона.

Уведомление направляется в виде документа на бумажном носителе или в форме электронного документа и подписывается уполномоченным лицом Банка. Уведомление о намерении осуществлять трансграничную передачу персональных данных должно содержать следующие сведения:

1) наименование, адрес Банка, а также дата и номер уведомления о намерении осуществлять обработку персональных данных, ранее направленного Банком в соответствии со статьей 22 Федерального закона;

2) наименование (фамилия, имя, отчество) лица, ответственного за организацию обработки персональных данных, номера контактных телефонов, почтовые адреса и адреса электронной почты;

3) правовое основание и цель трансграничной передачи персональных данных и дальнейшей обработки переданных персональных данных;

4) категории и перечень передаваемых персональных данных;

5) категории субъектов персональных данных, персональные данные которых передаются;

6) перечень иностранных государств, на территории которых планируется трансграничная передача персональных данных;

7) дата проведения Банком оценки соблюдения органами власти иностранных государств, иностранными физическими лицами, иностранными юридическими лицами, которым планируется трансграничная передача персональных данных, конфиденциальности персональных данных и обеспечения безопасности персональных данных при их обработке.

Банк до подачи уведомления обязан получить от органов власти иностранного государства, иностранных физических лиц, иностранных юридических лиц, которым планируется трансграничная передача персональных данных, следующие сведения:

1) сведения о принимаемых органами власти иностранного государства, иностранными физическими лицами, иностранными юридическими лицами, которым планируется трансграничная передача персональных данных, мерах по защите передаваемых персональных данных и об условиях прекращения их обработки;

2) информация о правовом регулировании в области персональных данных иностранного государства, под юрисдикцией которого находятся органы власти иностранного государства, иностранные физические лица, иностранные юридические лица, которым планируется трансграничная передача персональных данных (в случае, если предполагается осуществление трансграничной передачи персональных данных органам власти иностранного государства, иностранным физическим лицам, иностранным юридическим лицам, находящимся под юрисдикцией иностранного государства, не являющегося стороной Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных и не включенного в перечень иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных);

3) сведения об органах власти иностранного государства, иностранных физических лицах, иностранных юридических лицах, которым планируется трансграничная передача персональных данных (наименование либо фамилия, имя и отчество, а также номера контактных телефонов, почтовые адреса и адреса электронной почты).

В целях оценки достоверности сведений, содержащихся в уведомлении Банка о своем намерении осуществлять трансграничную передачу персональных данных, сведения, предоставляются Банком по запросу уполномоченного органа по защите прав субъектов персональных данных в течение десяти рабочих дней с даты получения такого запроса. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления Банком в адрес уполномоченного органа по защите прав субъектов персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

Трансграничная передача персональных данных 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, защиты экономических и финансовых интересов

Российской Федерации, обеспечения дипломатическими и международно-правовыми средствами защиты прав, свобод и интересов граждан Российской Федерации, суверенитета, безопасности, территориальной целостности Российской Федерации и других ее интересов на международной арене с даты принятия уполномоченным органом по защите прав субъектов персональных данных решения.

Решение о запрещении или об ограничении трансграничной передачи персональных данных в целях защиты нравственности, здоровья, прав и законных интересов граждан принимается уполномоченным органом по защите прав субъектов персональных данных по результатам рассмотрения уведомления. Такое решение принимается уполномоченным органом по защите прав субъектов персональных данных в течение десяти рабочих дней с даты поступления уведомления в порядке, установленном Правительством Российской Федерации. В случае направления уполномоченным органом по защите прав субъектов персональных данных запроса в Банк рассмотрение такого уведомления приостанавливается до даты предоставления оператором запрошенной информации.

После направления уведомления Банк вправе осуществлять трансграничную передачу персональных данных на территории указанных в таком уведомлении иностранных государств, являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных или включенных Перечень иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных (далее – Перечень), до принятия решения.

После направления уведомления Банк до истечения указанных выше сроков не вправе осуществлять трансграничную передачу персональных данных на территории указанных в уведомлении иностранных государств, не являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных и не включенных в Перечень, за исключением случая, если такая трансграничная передача персональных данных необходима для защиты жизни, здоровья, иных жизненно важных интересов субъекта персональных данных или других лиц.

Решение о запрещении или об ограничении трансграничной передачи персональных данных принимается уполномоченным органом по защите прав субъектов персональных данных в целях:

1) защиты основ конституционного строя Российской Федерации и безопасности государства - по представлению федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности;

2) обеспечения обороны страны - по представлению федерального органа исполнительной власти, уполномоченного в области обороны;

3) защиты экономических и финансовых интересов Российской Федерации - по представлению федеральных органов исполнительной власти, уполномоченных Президентом Российской Федерации или Правительством Российской Федерации;

4) обеспечения дипломатическими и международно-правовыми средствами защиты прав, свобод и интересов граждан Российской Федерации, суверенитета, безопасности, территориальной целостности Российской Федерации и других ее интересов на международной арене - по представлению федерального органа исполнительной власти, осуществляющего функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере международных отношений Российской Федерации.

Такое решение о запрещении или об ограничении трансграничной передачи персональных данных принимается уполномоченным органом по защите прав субъектов персональных данных в течение пяти рабочих дней с даты поступления соответствующего представления. Порядок принятия такого решения и порядок информирования операторов о принятом решении устанавливаются Правительством Российской Федерации.

В случае принятия уполномоченным органом по защите прав субъектов персональных данных решения о запрещении или об ограничении трансграничной передачи персональных данных Банк обязан обеспечить уничтожение органом власти иностранного государства, иностранным физическим лицом, иностранным юридическим лицом ранее переданных им персональных данных.

12. Хранение и защита персональных данных

Банк при обработке ПДн принимает необходимые правовые, организационные и технические меры или обеспечивает их принятие для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн.

Обеспечение безопасности персональных данных достигается:

1) определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

2) применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

3) применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

4) оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

5) учетом машинных носителей персональных данных;

6) обнаружением фактов несанкционированного доступа к персональным данным и принятием мер, в том числе мер по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные системы персональных данных и по реагированию на компьютерные инциденты в них;

7) восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

8) установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

9) контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

ПДн субъекта хранятся в подразделении Банка, которое отвечает за взаимодействие с субъектом ПДн, в личном деле субъекта ПДн, а также в электронном виде в информационной системе Банка. Личные дела хранятся в бумажном виде в папках, доступ к которым осуществляется в порядке, исключающем к ним доступ третьих лиц.

Руководители структурных подразделений, в которых происходит обработка ПДн, обеспечивают защиту и конфиденциальность ПДн, обрабатываемых в их подразделениях.

Исключается фиксация на одном материальном носителе ПДн и иных видов информационных активов, а также ПДн, цели обработки, которых заведомо несовместимы.

Использование и хранение биометрических ПДн вне ИСПДн предусмотрено осуществлять только на таких материальных носителях информации и с применением такой технологии ее хранения, которые обеспечивают защиту этих данных от неправомерного или случайного доступа к ним, их уничтожения, изменения,

блокирования, копирования, предоставления, распространения.

Хранение ПДн осуществляется в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен федеральным законом, 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 федеральным законом.

При обработке в Банке ПДн на бумажных носителях, в частности, при использовании Банком типовых форм документов, характер информации в которых предполагает или допускает включение в них ПДн, соблюдаются требования приложения 4 настоящего Положения, Постановления Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

Организационные и технические меры по обеспечению безопасности ПДн при их обработке с использованием средств автоматизации реализуются в Банке с учетом требований Постановления Правительства РФ № 1119, Приказа ФСТЭК РФ от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», ГОСТ Р 57580.1-2017.

13. Передача ПД

Сотрудники Банка, ответственные за работу с ПДн, должны четко знать случаи, при которых они могут передать информацию о субъекте ПДн запрашиваемым лицам. К таким случаям, как правило, относят запросы о получении информации, направленные государственными органами.

К числу потребителей ПДн субъектов вне Банка можно отнести государственные и негосударственные структуры, в том числе:

- правоохранительные органы;
- органы прокуратуры и ФСБ;
- налоговые инспекции;
- органы лицензирования и сертификации;
- страховые агентства;
- военкоматы;
- органы статистики;
- органы социального страхования;
- пенсионные фонды;
- подразделения муниципальных органов управления;
- Банк России и другие.

В случае если лицо, обратившееся с запросом, не уполномочено действующим законодательством Российской Федерации на получение ПДн субъекта, либо отсутствует письменное согласие субъекта на предоставление его ПДн, Банк обязан отказать в предоставлении ПДн. Лицу, обратившемуся с запросом, выдается письменное уведомление об отказе в предоставлении ПДн с указание причины отказа.

Не допускается сообщать ПДн субъекта в коммерческих целях без его письменного согласия.

Трансграничная передача ПДн осуществляется в соответствии с разделом 11 настоящего Положения.

14. Прекращение обработки и уничтожения ПДн

Банк должен прекратить обработку ПДн и их уничтожить либо обезличить в сроки, установленные Федеральным законом в следующих случаях:

А) В случае выявления неправомерной обработки ПДн при обращении субъекта ПДн или его представителя либо по запросу субъекта ПДн или его представителя либо уполномоченного органа по защите прав субъектов ПДн Банк обязан осуществить блокирование неправомерно обрабатываемых ПДн, относящихся к этому субъекту ПДн, или обеспечить их блокирование (если обработка ПДн осуществляется другим лицом, действующим по поручению Банка) с момента такого обращения или получения указанного запроса на период проверки. В случае выявления неточных ПДн при обращении субъекта ПДн или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов ПДн Банк обязан осуществить блокирование ПДн, относящихся к этому субъекту ПДн, или обеспечить их блокирование (если обработка ПДн осуществляется другим лицом, действующим по поручению Банка) 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.

Б) В случае подтверждения факта неточности ПДн Банк на основании сведений, представленных субъектом ПДн или его представителем либо уполномоченным органом по защите прав субъектов ПДн, или иных необходимых документов обязан уточнить ПДн либо обеспечить их уточнение (если обработка ПДн осуществляется другим лицом, действующим по поручению Банка) в течение семи рабочих дней со дня представления таких сведений и снять блокирование ПДн.

В) В случае выявления неправомерной обработки ПДн, осуществляемой Банком или лицом, действующим по поручению Банка, Банк в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку ПДн или обеспечить прекращение неправомерной обработки ПДн лицом, действующим по поручению Банка. В случае, если обеспечить правомерность обработки ПДн невозможно, Банк в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки ПДн, обязан уничтожить такие ПДн или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении ПДн Банк обязан уведомить субъекта ПДн или его представителя, а в случае, если обращение субъекта ПДн или его представителя либо запрос уполномоченного органа по защите прав субъектов ПДн были направлены уполномоченным органом по защите прав субъектов ПДн, также указанный орган.

В случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) ПДн, повлекшей нарушение прав субъектов ПДн, Банк обязан с момента выявления такого инцидента Банком, уполномоченным органом по защите прав субъектов персональных данных или иным заинтересованным лицом уведомить уполномоченный орган по защите прав субъектов персональных данных:

- в течение двадцати четырех часов о произошедшем инциденте, о предполагаемых причинах, повлекших нарушение прав субъектов ПДн, и предполагаемом вреде, нанесенном правам субъектов ПДн, о принятых мерах по устранению последствий соответствующего инцидента, а также предоставить сведения о лице, уполномоченном Банком на взаимодействие с уполномоченным органом по защите прав субъектов ПДн, по вопросам, связанным с выявленным инцидентом;

- в течение семидесяти двух часов о результатах внутреннего расследования выявленного инцидента, а также предоставить сведения о лицах, действия которых стали причиной выявленного инцидента (при наличии).

Г) В случае достижения цели обработки ПДн Банк обязан прекратить обработку ПДн или обеспечить ее прекращение (если обработка ПДн осуществляется другим лицом, действующим по поручению Банка) и уничтожить ПДн или обеспечить их уничтожение (если обработка ПДн осуществляется другим лицом, действующим по поручению Банка) в срок, не превышающий тридцати дней 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 федеральными законами.

Д) В случае отзыва субъектом ПДн данных согласия на обработку его ПДн Банк обязан прекратить их обработку или обеспечить прекращение такой обработки (если обработка ПДн осуществляется другим лицом, действующим по поручению Банка) и в случае, если сохранение ПДн более не требуется для целей обработки ПДн, уничтожить ПДн или обеспечить их уничтожение (если обработка ПДн осуществляется другим лицом, действующим по поручению Банка) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, 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 федеральными законами.

В случае обращения субъекта ПДн к Банку с требованием о прекращении обработки ПДН Банк обязан в срок, не превышающий десяти рабочих дней с даты получения Банком соответствующего требования, прекратить их обработку или обеспечить прекращение такой обработки (если такая обработка осуществляется лицом, осуществляющим обработку ПДн), за исключением случаев, предусмотренных пунктами 2 - 11 части 1 статьи 6, частью 2 статьи 10 и частью 2 статьи 11 Федерального закона. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления Банком в адрес субъекта ПДн мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

Е) В случае отсутствия возможности уничтожения ПДн в течение срока, указанного в подпунктах В – Д настоящего раздела Положения, Банк осуществляет блокирование таких ПДн или обеспечивает их блокирование (если обработка ПДн осуществляется другим лицом, действующим по поручению Банка) и обеспечивает уничтожение ПДн в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

Ж) Подтверждение уничтожения персональных данных осуществляется с учетом требований приказа Роскомнадзора от 28.10.2022 № 179 «Об утверждении Требований к подтверждению уничтожения персональных данных».

Уничтожение ПДн на бумажных носителях, находящихся на хранении в архиве, по истечении сроков архивного хранения осуществляется в соответствии с Инструкцией по делопроизводству Банка.

Уничтожение ПДн до истечения сроков архивного хранения (отзыв субъектом ПДн согласия на обработку его ПДн или выявления неправомерной обработки ПДн), происходит с письменного разрешения на уничтожение по представляемому списку ПДн лица ответственного за обеспечение безопасности ПДн в Банке. Уничтожение ПДн производится уполномоченным работником структурного подразделения в присутствии двух других работников Банка. При этом составляется «Акт уничтожения персональных данных» (приложение 5 настоящего Положения) и подписывается членами комиссии по приведению Банка в соответствие с требованиями Федерального закона, при необходимости делается отметка в «Журнале учета носителей персональных данных». Уничтожение ПДн без оформления соответствующих актов не допускается.

Уничтожение ПДн на бумажных носителях производится путем их резки на бумагорезательной машине или сжигания. Уничтожение ПДн на электронных носителях производится путем ее стирания с использованием специальных средств (способом, исключающим возможность восстановления ПДн), при необходимости с последующим уничтожением материального носителя.

15. Права субъектов ПДн

Субъект ПДн имеет право на получение следующих сведений:

1) подтверждение факта обработки персональных данных оператором;

2) правовые основания и цели обработки персональных данных;

3) цели и применяемые оператором способы обработки персональных данных;

4) 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;

5) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

6) сроки обработки персональных данных, в том числе сроки их хранения;

7) порядок осуществления субъектом персональных данных прав, предусмотренных настоящим Федеральным законом;

8) информацию об осуществленной или о предполагаемой трансграничной передаче данных;

9) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;

9.1) информацию о способах исполнения оператором обязанностей, установленных статьей 18.1 Федерального закона;

10) иные сведения, предусмотренные настоящим Федеральным законом или другими федеральными законами.

Сведения, должны быть предоставлены субъекту ПДн Банком в доступной форме, и в них не должны содержаться ПДн, относящиеся к другим субъектам ПДн, за исключением случаев, если имеются законные основания для раскрытия таких ПДн.

Субъект ПДн вправе требовать от Банка уточнения его ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

Сведения предоставляются субъекту ПДн или его представителю Банком в течение десяти рабочих дней с момента обращения либо получения оператором запроса субъекта ПДн или его представителя. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления Банком в адрес субъекта ПДн мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта ПДн или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта ПДн в отношениях с Банком (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки ПДн Банком, подпись субъекта ПДн или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации. Банк предоставляет сведения, указанные в подпунктах 1 - 10 абзаца 1 раздела 15 настоящего Положения, субъекту ПДн или его представителю в той форме, в которой направлены соответствующие обращение либо запрос, если иное не указано в обращении или запросе.

В случае, если сведения об обработке ПДн и ПДн были предоставлены для ознакомления субъекту ПДн по его запросу, субъект ПДн вправе обратиться повторно в Банк или направить повторный запрос в целях получения сведений и ознакомления с ПДн не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом,

принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн.

Субъект ПДн вправе обратиться повторно в Банк или направить повторный запрос в целях получения сведений об обработке его ПДн в Банке, а также в целях ознакомления с обрабатываемыми ПДн до истечения срока в тридцать дней после первоначального обращения или направления первоначального запроса, если такие сведения и (или) обрабатываемые ПДн не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос дополнительно должен содержать обоснование направления повторного запроса.

Банк вправе отказать субъекту ПДн в выполнении повторного запроса, не соответствующего условиям, частей 4 и 5 статья 14 Федерального закона. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на Банке.

Право субъекта ПДн на доступ к его ПДн может быть ограничено в соответствии с федеральными законами.

Обработка ПДн в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи допускается только при условии предварительного согласия субъекта ПДн. Указанная обработка ПДн признается осуществляемой без предварительного согласия субъекта ПДн, если Банк не докажет, что такое согласие было получено. Банк обязан немедленно прекратить по требованию субъекта ПДн обработку его ПДн в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи.

Если субъект персональных данных считает, что Банк осуществляет обработку его персональных данных с нарушением требований настоящего Федерального закона или иным образом нарушает его права и свободы, субъект ПДн вправе обжаловать действия или бездействие Банка в уполномоченный орган по защите прав субъектов ПДн или в судебном порядке.

Субъект ПДн имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

16. Права и обязанности банка

16.1. При сборе ПДн Банк обязан предоставить субъекту ПДн по его просьбе информацию, предусмотренную подпунктами 1 – 10 абзаца 1 раздела 15 настоящего Положения.

16.2. Если в соответствии с федеральным законом предоставление ПДн и (или) получение Банком согласия на обработку ПДн являются обязательными, Банк обязан разъяснить субъекту ПДн юридические последствия отказа предоставить его ПДн и (или) дать согласие на их обработку.

16.3. Если ПДн получены не от субъекта ПДн, Банк, за исключением случаев, предусмотренных пунктом 16.4 настоящего раздела, до начала обработки ПДн обязан предоставить субъекту ПДн следующую информацию:

1) наименование либо фамилия, имя, отчество и адрес оператора или его представителя;

2) цель обработки персональных данных и ее правовое основание;

2.1) перечень персональных данных;

3) предполагаемые пользователи персональных данных;

4) установленные настоящим Федеральным законом права субъекта персональных данных;

5) источник получения персональных данных.

Типовая форма уведомления приведена в приложении 6 настоящего Положения.

16.4 Банк освобождается от обязанности предоставить субъекту ПДн сведения, предусмотренные в пункте 16.3 настоящего раздела, в случаях, если:

1) субъект ПДн уведомлен об осуществлении обработки его ПДн Банком;

2) ПДн получены Банком на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн;

3) обработка ПДн, разрешенных субъектом ПДн для распространения, осуществляется с соблюдением запретов и условий, предусмотренных статьей 10.1 Федерального закона;

4) Банк осуществляет обработку ПДн для статистических или иных исследовательских целей, для осуществления профессиональной деятельности журналиста либо научной, литературной или иной творческой деятельности, если при этом не нарушаются права и законные интересы субъекта ПДн;

5) предоставление субъекту ПДн сведений, предусмотренных пунктом 16.2 настоящего раздела, нарушает права и законные интересы третьих лиц.

16.5. Банку запрещается принятие на основании исключительно автоматизированной обработки ПДн решений, порождающих юридические последствия в отношении субъекта ПДн или иным образом затрагивающих его права и законные интересы, за исключением случаев, наличия согласия в письменной форме субъекта ПДн или в случаях, предусмотренных федеральными законами, устанавливающими также меры по обеспечению соблюдения прав и законных интересов субъекта ПДн.

Банк обязан разъяснить субъекту ПДн порядок принятия решения на основании исключительно автоматизированной обработки его ПДн и возможные юридические последствия такого решения, предоставить возможность заявить возражение против такого решения, а также разъяснить порядок защиты субъектом ПДн своих прав и законных интересов.

Банк обязан рассмотреть возражение в течение тридцати дней со дня его получения и уведомить субъекта персональных данных о результатах рассмотрения такого возражения.

16.6. Обязанности Банка при обращении к нему субъекта ПДн либо при получении запроса субъекта ПДн или его представителя, а также уполномоченного органа по защите прав субъектов ПДн:

16.6.1. Банк обязан сообщить в порядке, предусмотренном статьей 14 Федерального закона, субъекту Пдн или его представителю информацию о наличии ПДн, относящихся к соответствующему субъекту ПДн, а также предоставить возможность ознакомления с этими ПДн при обращении субъекта ПДн или его представителя либо в течение десяти рабочих дней с даты получения запроса субъекта ПДн или его представителя. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления Банком в адрес субъекта ПДн мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

16.6.2. В случае отказа в предоставлении информации о наличии ПДн о соответствующем субъекте ПДн или ПДн субъекту ПДн или его представителю при их обращении либо при получении запроса субъекта ПДн или его представителя Банк обязан дать в письменной форме мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 Федерального закона или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий десяти рабочих дней со дня обращения субъекта ПДн или его представителя либо с даты получения запроса субъекта ПДн или его представителя. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления Банком в адрес субъекта ПДн мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

16.6.3. Банк обязан предоставить безвозмездно субъекту ПДн или его представителю возможность ознакомления с ПДн, относящимися к этому субъекту ПДн. В срок, не превышающий семи рабочих дней со дня предоставления субъектом ПДн или его представителем сведений, подтверждающих, что ПДн являются неполными, неточными или неактуальными, Банк обязан внести в них необходимые изменения. В срок, не превышающий семи рабочих дней со дня представления субъектом ПДн или его представителем сведений, подтверждающих, что такие ПДн являются незаконно полученными или не являются необходимыми для заявленной цели обработки, Банк обязан уничтожить такие ПДн. Банк обязан уведомить субъекта ПДн или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым ПДн этого субъекта были переданы.

16.6.4. Банк обязан сообщить в уполномоченный орган по защите прав субъектов персональных данных по запросу этого органа необходимую информацию в течение десяти рабочих дней с даты получения такого запроса. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления Банком в адрес уполномоченного органа по защите прав субъектов персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

16.6.5. Банк принимает меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами. Банк самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено Федеральным законом или другими федеральными законами. К таким мерам, в частности, относятся:

1) назначение ответственного за организацию обработки персональных данных приказом Банка;

2) издание Банком документов, определяющих политику Банка в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, определяющих для каждой цели обработки персональных данных категории и перечень обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, способы, сроки их обработки и хранения, порядок уничтожения персональных данных при достижении целей их обработки или при наступлении иных законных оснований, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений. Такие документы и локальные акты не могут содержать положения, ограничивающие права субъектов персональных данных, а также возлагающие на операторов не предусмотренные законодательством Российской Федерации полномочия и обязанности;

3) применение правовых, организационных и технических мер по обеспечению безопасности персональных данных;

4) осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных Федеральному закону и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике Банка в отношении обработки персональных данных, локальным актам Банка с учетом Стандарта Банка России СТО БР ИББС-1.2-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0-2014»;

5) оценку вреда в соответствии с требованиями, установленными уполномоченным органом по защите прав субъектов персональных данных, который может быть причинен субъектам персональных данных в случае нарушения настоящего Федерального закона,

соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных настоящим Федеральным законом, с учетом рекомендаций в области стандартизации Банка России РС БР ИББС-2.2-2009 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков нарушения информационной безопасности»;

6) ознакомление работников Банка, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику Банка в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и обучение указанных работников.

Банк обеспечивает неограниченный доступ к документу, определяющему его политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных. Банк опубликовывает в информационно-телекоммуникационной сети «Интернет», в том числе на страницах принадлежащего Банку официального сайта http://www.doncombank.ru (далее – сайт Банка), с использованием которых осуществляется сбор персональных данных, в том числе, документ, определяющий его политику в отношении обработки персональных данных, и сведения о реализуемых требованиях к защите персональных данных, а также обеспечивает возможность доступа к указанному документу с использованием средств сети «Интернет». Банк осуществляет информирование посетителей сайта Банка о факте сбора их персональных данных, в том числе посредством программного модуля Yandex.Metrika, на страницах сайта Банка, с использованием которых осуществляется сбор персональных данных. Форма Согласия на обработку персональных данных для посетителей сайта установлена в Приложении 7 настоящего Положения.

Банк обязан представить документы и локальные акты, указанные в настоящем пункте Положения, и (или) иным образом подтвердить принятие мер, указанных в настоящем подпункте Положения, по запросу уполномоченного органа по защите прав субъектов персональных данных.

17. Ответственность

Лица, виновные в нарушении норм, регулирующих обработку и защиту ПДн, установленных действующим законодательством, несут дисциплинарную, административную, гражданскую, уголовную или иную ответственность в соответствии с действующим законодательством Российской Федерации.

Руководители подразделений, в которых происходит обработка ПДн, несут персональную ответственность за обеспечение защиты обрабатываемых и хранящихся в их подразделениях.

Каждый сотрудник Банка, участвующий в рамках своих функциональных обязанностей в процессах обработки ПДн и другой конфиденциальной информации, несет персональную ответственность за свои действия при работе в ИС Банка.

В случае, если Банк поручает обработку ПДн другому лицу, ответственность перед субъектом ПДн за действия указанного лица несет Банк. Лицо, осуществляющее обработку ПДн по поручению Банка, несет ответственность перед Банком.

В случае, если Банк поручает обработку ПДн иностранному физическому лицу или иностранному юридическому лицу, ответственность перед субъектом ПДн за действия указанных лиц несет Банк и лицо, осуществляющее обработку ПДн по поручению Банка.

Приложение 1

ИНСТРУКЦИЯ
пользователя при обработке персональных данных в информационной системе ПАО «Донкомбанк»

1. Общие положения

1.1. Настоящая инструкция определяет права, обязанности и ответственность пользователей, допущенных к обработке персональных данных (далее – ПДн) в информационной системе ПАО «Донкомбанк» (далее – ИС Банка). Также инструкция определяет функции, задачи и порядок эксплуатации пользователями программного обеспечения и средств вычислительной техники (далее - СВТ), на которых ведется обработка ПДн, входящих в состав ИС Банка.

1.2. Пользователями информационных систем персональных данных (далее - ИСПДн) являются работники Банка, допущенные к обработке ПДн согласно утвержденному Перечню.

1.3. Перед началом работ пользователь должен ознакомиться с содержанием следующих документов:

- Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;
- эксплуатационной документацией на ИСПДн и средства защиты информации;
- нормативными и организационно-распорядительными документами Банка в области защиты ПДн.

1.4. Оперативный контроль за действиями пользователей при работе в ИСПДн осуществляет администратор по обеспечению безопасности ИСПДн (далее – Администратор), который имеет право приостановить обработку информации в случае выявления нарушений.

1.5. Каждый сотрудник Банка, участвующий в рамках своих функциональных обязанностей в процессах обработки ПДн и другой конфиденциальной информации, несет персональную ответственность за свои действия при работе в ИС Банка.

II. Обеспечение информационной безопасности

2.1. Пользователю ИС Банка предоставляется соответствующий его полномочиям доступ к ИСПДн и ресурсам (сетевым дискам, каталогом, файлам, принтеру, коммуникационным портам).

2.2. Все сотрудник Банка обладают уникальными учетными записями для доступа в ИС Банка и для каждой ИСПДн.

2.3. Устройства отображения и вывода информации (дисплей, принтер) в процессе эксплуатации ИСПДн должны устанавливаться с учетом исключения несанкционированного доступа к выводимой информации лицами, не имеющими к ней соответствующего допуска. В случае невозможности выполнения указанных требований по размещению технических средств ИСПДн, должны приниматься дополнительные организационные и технические меры по исключению несанкционированного доступа к информации.

2.4. При эксплуатации ИСПДн должно быть обеспечено непрерывное функционирование установленных средств защиты информации и антивирусного программного обеспечения.

2.5. В процессе работы с ПДн должны использоваться исключительно штатные технические средства ИСПДн.

2.6. Внесение пользователем самостоятельных изменений в аппаратно-программную конфигурацию ИС Банка категорически запрещено.

III. Права и обязанности пользователя

3.1. Пользователь обязан:

- выполнять требования настоящей инструкции, а также требования организационно-технических и распорядительных документов в области защиты ПДн;
- действовать в соответствии с инструкцией (руководством, регламентом и т.п.), входящей в состав эксплуатационной документации на ИСПДн;
- соблюдать правила работы со средствами защиты информации, установленными в ИСПДн, согласно утвержденной инструкции по использованию и заводскому руководству пользователей по эксплуатации этих средств;
- докладывать Администратору о фактах нарушения требований инструкций по обеспечению защиты информации;
- знать штатные режимы работы программного обеспечения;
- использовать доступные защитные механизмы для обеспечения конфиденциальности и целостности своей информации;
- помнить личные пароли и идентификаторы, персональные идентификаторы не оставлять без присмотра и хранить в запирающемся ящике стола или сейфе;
- не допускать использования в ИСПДн неучтенных машинных носителей (флеш-дисков, CD, DVD, дискет);
- при поступлении необходимой для работы информации на неучтенных электронных носителях из сторонних организаций, перед началом работы провести их проверку на предмет наличия компьютерных вирусов;
- оповещать непосредственного начальника и Администратора о всех фактах или попытках несанкционированного доступа к информации, обрабатываемой в ИС Банка;
- незамедлительно, в кратчайшие сроки, сообщать непосредственному руководителю об утрате или недостаче носителей информации, удостоверений, пропусков, ключей от помещений, хранилищ, сейфов, личных печатей и о других фактах, которые могут привести к разглашению ПДн;
- не сообщать устно или письменно, не передавать в каком либо виде третьим лицам и не раскрывать публично ПДн без соответствующего разрешения непосредственного руководителя;
- соблюдать правила внутренних документов при работе в сетях связи общего пользования и (или) сетях международного информационного обмена.

3.2. Пользователь имеет право:

- использовать штатные программно-аппаратные средства ИСПДн для решения профессиональных задач;
- обращаться к Администратору с просьбой об оказании технической и методической помощи в работе по обеспечению безопасности информации;
- обращаться к Администратору с требованием о прекращении обработки ПДн в случаях нарушения установленной технологии обработки информации или выхода из строя средств защиты.

3.3. Пользователю запрещается:

- разглашать сведения о применяемых средствах защиты ПДн и содержание документов лицам, не имеющим отношения к проводимым работам;
- удалять с обрабатываемых или распечатываемых документов пометки конфиденциальности;
- использовать в ИСПДн неучтенные машинные носители информации или не предназначенные для хранения ПДн каталоги рабочих станций;
- использовать учтенные служебные машинные носители информации для хранения информации, не имеющей отношения к выполняемым работам;
- оставлять учтенные служебные машинные носители информации и документы бесконтрольно;

- оставлять свое рабочее место без присмотра, предварительно не заблокировав (штатными средствами операционной системы Windows– комбинацией клавиш [WIN] + [L] или [CTRL] + [ALT] + [DEL] с дальнейшим нажатием кнопки «Блокировка» появившегося меню, либо при помощи штатных средств защиты информации от несанкционированного доступа при их наличии);
- самовольно изменять состав и конфигурацию используемых программных, аппаратных, программно-аппаратных средств, самовольно устанавливать программное обеспечение, отключать/подключать оборудование или изменять режимы его работы.
- разрабатывать и/или использовать программы, с помощью которых можно получить несанкционированный доступ к ПДн, разработка и использование которых квалифицируется как попытка преднамеренного несанкционированного доступа к обрабатываемым данным;
- изменять или тиражировать установленное в ИСПДн программное обеспечение;
- фиксировать на любых носителях персональный пароль;
- передавать персональный идентификатор сторонним лицам или разрешать посторонним лицам работать под своей учетной записью на СВТ;
- проводить обработку информации в ИСПДн при неработоспособных или отключенных средствах защиты информации;
- осуществлять обработку персональных данных в условиях, позволяющих осуществлять их просмотр лицами, не имеющими к ним допуска, а также при несоблюдении требований по эксплуатации СВТ;
- пересылать конфиденциальную информацию (в том числе ПДн) по каналам связи в открытом виде, в том числе интернет, по телефону, факсу, электронной почте и т.п. (без использования средств шифрования или шифрования и электронной подписи).

IV. Ответственность пользователя

4.1. Пользователь отвечает за соблюдение правил эксплуатации ИСПДн, сохранность информации, документов и электронных носителей информации, с которыми он работает.

4.2. Пользователь несет персональную ответственность за:

- соблюдение установленных требований по безопасности информации при обработке, копировании (уничтожении) ПДн;
- использование неучтенных электронных носителей информации;
- несоблюдение правил использования электронных носителей информации, поступающих из сторонних организаций;
- правильность и полноту выполнения целей, задач, функций, прав и обязанностей, возложенных на него;
- сохранность сведений ограниченного распространения в соответствии с требованиями законодательства в области защиты ПДн;
- выполнение указаний Администратора, касающихся работы в ИСПДн и защиты информации;
- обеспечение сохранности и неразглашение сведений о парольной защите ИСПДн;
- соблюдение технологии обработки защищаемой информации, неизменность условий обработки информации (размещение и/или состав технических средств обработки и защиты информации, состав используемого в ИСПДн программного обеспечения) в соответствии с организационно-технической документацией на ИСПДн;
- неисполнение или ненадлежащее исполнение обязанностей, предусмотренных настоящей инструкцией, в пределах, установленных законодательством Российской Федерации, а также за действия (бездействия), нарушающие права и законные интересы граждан и юридических лиц.

Приложение 2

Правила доступа в помещения, где ведется обработка персональных данных.

1. Настоящие правила определяют порядок ограничения доступа сотрудников и посетителей в помещения Банка, где ведется обработка персональных данных (далее - ПДн). Ограничение доступа в помещения устанавливается с целью исключения фактов неправомерного или случайного доступа к ПДн, уничтожения, изменения, блокирования, копирования, распространения ПДн, а также от иных неправомерных действий.
2. В помещениях, в которых ведется обработка ПДн, должна быть исключена возможность бесконтрольного проникновения посторонних лиц и обеспечена сохранность находящихся в этих помещениях документов и средств автоматизации.
3. Доступ посетителей в помещения разрешается только в рабочее время в присутствии сотрудника структурного подразделения, ведущего обработку ПДн.
4. Уборка помещений, в которых ведется обработка ПДн, должна производиться в присутствии сотрудника структурного подразделения, ведущего обработку ПДн, с соблюдением мер, исключающих доступ посторонних лиц к ПДн.
5. Обслуживание технических средств, находящихся в помещении, где ведется обработка ПДн, должна производиться под наблюдением сотрудника структурного подразделения, ведущего обработку ПДн.
6. Входные двери оборудуются замками, гарантирующими надежное закрытие помещений в нерабочее время.
7. Ключи от помещений выдаются под роспись сотрудникам Банка и сдаются на пост охраны в конце рабочего дня (кроме зав. сектором по работе с кадрами).
8. Все помещения оборудуются контрольными датчиками на открытие двери, а прилегающие коридоры оборудуются датчиками движения.
9. Окна помещений оборудуются охранной сигнализацией, а окна первых этажей также оборудуются металлическими решетками, препятствующими несанкционированному доступу в помещения.
10. Для хранения материальных носителей ПДн помещения снабжаются сейфами и специальными шкафами.
11. В помещениях, где ведется обработка ПДн, должна соблюдаться «политика чистого стола» (после завершения работы с документами, содержащими ПД, их необходимо убрать со стола в защищенное место).
12. Категорически запрещен бесконтрольный доступ посетителей Банка в помещения, где ведется отработка ПДн.
13. Постановка на охрану и снятие с охраны помещений Банка, в том числе, где ведется обработка ПДн, осуществляется в соответствии с «Инструкцией об организации охраны объектов банка техническими средствами охранно - пожарной и тревожной сигнализации».

Приложение 3

Согласие на обработку персональных данных (типовая форма)[1]

Я, _____,
(Ф.И.О.)

проживающий(ая) по адресу:_____
(номер паспорта или иного основного документа, удостоверяющего личность, сведения о дате его выдачи и выдавшем его органе)

_____

в лице _____
(Ф.И.О., адрес, данные паспорта (или иного документа, удостоверяющего личность) представителя субъекта персональных данных)

_____,

действующего на основании _____
(реквизиты доверенности или иного документа, подтверждающего полномочия представителя субъекта персональных данных)

_____,

в соответствии с Федеральным законом Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных» даю свое согласие ПАО «Донкомбанк» г. Ростов-на-Дону, пр. Михаила Нагибина, д. 32а (далее - Банк) на обработку моих персональных данных.

Персональные данные предоставляются Банку с целью

_____
(цель обработки персональных данных)

_____.

Под персональными данными, на обработку которых дается согласие, я понимаю:

_____
(перечень персональных данных)

_____.

Персональные данные могут быть переданы_____

_____
(наименование или фамилия, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Банка, если обработка будет поручена такому лицу)

Под обработкой персональных данных я понимаю:

_____
(сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ (в том числе при поручении обработки персональных данных третьим лицам, указанным выше), обезличивание, блокирование, удаление, уничтожение, а также копирование (электронно/на бумажном носителе) документа, удостоверяющего личность, и других документов, по которым проводилась идентификация, в том числе с моим фотографическим изображением/без моего фотографического изображения, трансграничную передачу моих персональных данных с использованием и без использования средств автоматизации)

_____.

Настоящее Согласие действует в течение_____.
(указать срок действия согласия)

Настоящее Согласие может быть отозвано мной путем направления письменного заявления в Банк. В случае отзыва мной настоящего Согласия Банк вправе продолжить обработку мои персональных данных без моего согласия при наличии оснований, установленных законодательством Российской Федерации.

“____” _____ 20___ г. _____ _____
(подпись) (Ф.И.О.)

[1] Конкретные формы Согласия на обработку персональных данных устанавливаются внутренними нормативными документами в соответствии с видами деятельности, предусмотренными учредительными документами ПАО «Донкомбанк».

Приложение 4

Правила обработки персональных данных осуществляемой без использования средств автоматизации

Обработка персональных данных (далее - ПДн), содержащихся в информационной системе персональных данных (далее - ИСПДн) либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с ПДн, как использование, уточнение, распространение, уничтожение ПДн в отношении каждого из субъектов ПДн, осуществляются при непосредственном участии человека.

Обработка ПД не может быть признана осуществляемой с использованием средств автоматизации только на том основании, что ПДн содержатся в ИСПДн либо были извлечены из нее.

При обработке ПДн, осуществляемой без использования средств автоматизации, должны выполняться следующие требования:

1. ПДн при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях ПДн (далее - материальные носители), в специальных разделах или на полях форм (бланков).

2. 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 должен использоваться отдельный материальный носитель.

3. Лица, осуществляющие обработку ПДн без использования средств автоматизации (сотрудники Банка или лица, осуществляющие такую обработку по договору с Банком), должны быть проинформированы о факте обработки ими ПДн, обработка которых осуществляется Банком без использования средств автоматизации, категориях обрабатываемых ПДн, а также об особенностях и правилах осуществления такой обработки.

4. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовая форма), должны соблюдаться следующие условия:

- типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки ПДн, осуществляемой без использования средств автоматизации, имя (наименование) и адрес Банка, 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;
- типовая форма должна предусматривать поле, в котором субъект ПДн может поставить отметку о своем согласии на обработку ПДн, осуществляемую без использования средств автоматизации, - при необходимости получения письменного согласия на обработку ПДн;
- типовая форма должна 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;
- типовая форма должна исключать объединение полей, предназначенных для внесения ПДн, цели обработки которых заведомо не совместимы.

5. При ведении журналов (реестров, книг), содержащих ПДн, необходимые для однократного пропуска субъекта ПДн на территорию Банка, или в иных аналогичных целях, должны соблюдаться следующие условия:

- необходимость ведения такого журнала (реестра, книги) должна быть предусмотрена локальными документами, содержащим сведения о цели обработки ПДн, осуществляемой без использования средств автоматизации, способы фиксации и состав информации, запрашиваемой у субъектов ПДн, перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги), сроки обработки ПДн, а также сведения о порядке пропуска субъекта ПДн на территорию Банка без подтверждения подлинности ПДн, сообщенных субъектом ПДн;
- копирование содержащейся в таких журналах (реестрах, книгах) информации не допускается;
- ПДн каждого субъекта ПДн могут заноситься в такой журнал (книгу, реестр) не более одного раза в каждом случае пропуска субъекта ПДн на территорию Банка.

6. При несовместимости целей обработки ПДн, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку ПДн отдельно от других зафиксированных на том же носителе ПДн, должны быть приняты меры по обеспечению раздельной обработки ПДн, в частности:

- при необходимости использования или распространения определенных ПДн отдельно от находящихся на том же материальном носителе других ПДн осуществляется копирование ПДн, подлежащих распространению или использованию, способом, исключающим одновременное копирование ПДн, не подлежащих распространению и использованию, и используется (распространяется) копия ПДн;
- при необходимости уничтожения или блокирования части ПДн уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование ПДн, подлежащих уничтожению или блокированию.

7. Уничтожение или обезличивание 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).

8. Требования, предусмотренные пунктами 6 и 7 настоящих Правил, применяются также в случае, если необходимо обеспечить раздельную обработку зафиксированных на одном материальном носителе ПДн и информации, не являющейся ПДн.

9. Уточнение ПДн при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными ПДн.

10. Обработка ПДн, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории ПДн можно было определить места хранения ПДн (материальных носителей) и установить перечень лиц, осуществляющих обработку ПДн либо имеющих к ним доступ.

11. Необходимо обеспечивать раздельное хранение ПДн (материальных носителей), обработка которых осуществляется в различных целях. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность ПДн и исключающие несанкционированный к ним доступ.

Приложение 5

Разрешаю уничтожить
<руководитель структурного подразделения
или должностное лицо, ответственное
за обеспечение безопасности
персональных данных>
ФИО

_____
«___» _____20__ г.

Акт об уничтожении персональных данных

Комиссия в составе:

	ФИО	Должность
Председатель		
Члены комиссии		

провела отбор носителей персональных данных и установила, что в соответствии с требованиями руководящих документов по защите информации ПАО «Донкомбанк» информация, записанная на них в процессе эксплуатации, подлежит уничтожению:

№ п/п	Дата	Тип носителя	Регистрационный номер носителя ПД	Примечание

Всего подлежит уничтожению носителей_____
(цифрами и прописью)

После утверждения акта перечисленные носители сверены с записями в акте и на указанных носителях персональные данные уничтожены путем

_____.
(стирания на устройстве гарантированного уничтожения информации и т.п.)

После утверждения акта перечисленные носители сверены с записями в акте и уничтожены путем

_____.
(разрезания, сжигания, механического уничтожения, сдачи предприятию по утилизации вторичного сырья и т.п.)

Уничтоженные носители с книг и журналов учета списаны.

Члены комиссии: _____ /_____/
_____ /_____/

Примечание:
1. Акт составляется раздельно на каждый способ уничтожения носителей.
2. Все листы акта, а так же все произведенные исправления и дополнения в акте заверяются подписями всех членов комиссии.

Приложение 6

Уведомление об обработке персональных данных

Уважаемый(ая) _____,
(Ф.И.О.)

в ПАО «Донкомбанк» (далее - Банк), расположенном по адресу г. Ростов-на-Дону, пр. Михаила Нагибина 32а, ведется обработка ваших персональных данных.

Ваши персональные данные были предоставлены Банку с целью _____
(цель обработки и ее правовое основание, источник получения персональных данных, перечень персональных данных)

Ваши данные будут обрабатываться сотрудниками Банка и/или будут переданы в _____
(наименование организации, в которую планируется передача данных)

Согласно Федеральному закону №152-ФЗ «О персональных данных», Вы имеете право на получение сведений о наличии у Банка ваших персональных данных и на ознакомление с такими персональными данными. Вы имеете право требовать от Банка уточнения ваших персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

Доступ к вашим персональным данным может быть предоставлен вам или вашему законному представителю при обращении либо при получении запроса от вас или вашего законного представителя. Запрос должен содержать: номер вашего основного документа, удостоверяющего личность или вашего законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие ваше участие в отношениях с Банком (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Банком, подпись ваша или вашего представителя. Запрос может быть направлен в электронной форме и подписан электронной цифровой подписью в соответствии с законодательством Российской Федерации.

«___ »_____20___ г.

_____	_____	_____
(должность)	(Ф.И.О.)	(подпись)

Приложение 7

Согласие на обработку персональных данных для посетителей сайта

Продолжая работу на сайте я выражаю свое согласие ПАО «Донкомбанк» (адрес: 344068, г. Ростов-на-Дону, пр. Михаила Нагибина, 32а) (далее – Банк) на автоматизированную обработку моих персональных данных (фамилия, имя, отчество, номер телефона, ИНН, адрес электронной почты, адрес места регистрации, паспортные данные, файлы cookie, сведения о действиях пользователя на сайте, сведения об оборудовании пользователя, дата и время сессии), в т.ч. с использованием метрической программы Яндекс.Метрика, с совершением действий: сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, обезличивание, блокирование, удаление, уничтожение, передача (предоставление, доступ). Обработка персональных данных осуществляется в целях улучшения работы сайта, совершенствования продуктов и услуг Банка, определения предпочтений пользователя, предоставления целевой информации по продуктам и услугам Банка.

Настоящее согласие действует с момента его предоставления и в течение всего периода использования сайта.

В случае отказа от обработки персональных данных, в том числе метрической программой я проинформирован о необходимости прекратить использование сайта или отключить файлы cookie в настройках браузера.

Условия и принципы обработки персональных данных

Банк очень серьезно относится к вопросам конфиденциальности и безопасности информации. Защита ваших персональных данных* - один из наших ключевых приоритетов.

Мы обрабатываем ваши персональные данные, собранные на законных основаниях и в рамках четко сформулированных целей, характерных для взаимодействия Банка со всеми сторонами:

- клиентами, потенциальными клиентами, их родственниками или представителями;
- контрагентами и партнерами (как существующими, так и потенциальными);
- сотрудниками (включая их родственников) и соискателями.

Мы можем собирать ваши персональные данные, информацию о предпочтениях, совершенных действиях и транзакциях и т.п. при помощи веб-сайта и мобильных приложений Банка для заранее определенных и законных целей.

Мы можем передавать ваши персональные данные, строго при соблюдении требований законодательства.

Мы уважаем ваши права и свободы, в частности, связанные с вопросами обработки ваших персональных данных.

С вопросами, связанными с обработкой персональных данных, обращайтесь по адресу rstdkb@aaanet.ru или телефону +7(863)2076060.

* Под термином «персональные данные» понимается любая информация, относящаяся к идентифицированному или идентифицируемому физическому лицу. В состав персональных данных могут входить фамилия, имя, отчество, номер телефона, ИНН, адрес электронной почты, адрес места регистрации, паспортные данные, а также другая информация, например, файлы cookie.