



**Публичное акционерное общество  
«Санкт-Петербургский Индустриальный Акционерный Банк»  
(ПАО БАНК «СИАБ»)**

УТВЕРЖДЕНО  
решением Правления ПАО БАНК «СИАБ»  
Протокол № 58 от 05.09.2023

**Положение  
о защите персональных данных**

**Санкт-Петербург  
2023 год**

## Оглавление

номер раздела	Наименование раздела	Стр.
1	Общие положения	3
2	Цели обработки персональных данных	6
3	Сбор и дальнейшая обработка персональных данных	6
4	Основные меры обеспечения защиты персональных данных	7
5	Порядок и условия обработки персональных данных сотрудников	7
6	Порядок и условия обработки биометрических персональных данных	9
7	Порядок обработки обращений субъектов персональных данных	10
8	Порядок доступа к персональным данным, передача уполномоченным государственным органам	10
9	Обязанности сотрудников	11
10	Права сотрудников в целях обеспечения защиты персональных данных, хранящихся в Банке	11
11	Организация контроля выполнения требований по защите персональных данных	12
12	Ответственность за нарушение требований по защите персональных данных	13
	Приложения	
	Приложение 1. Перечень персональных данных, обрабатываемых в Банке	14
	Приложение 2. Общие и частные цели обработки персональных данных	20
	Приложение 3. Правовое основание получения персональных данных, обрабатываемых в Банке	23
	Приложение 4. Текст согласия на обработку персональных данных (обязательная форма)	24
	Приложение 5. Формирование состава средств защиты персональных данных	26
	Приложение 6. Нормативные правовые акты, определяющие сроки архивного хранения документов, содержащих персональные данные, в Банк	27
	Приложение 7. Порядок обеспечения непрерывности и реагировании на инцидент при эксплуатации технических средств и программного обеспечения, баз данных и средств защиты информации ИСПДн	29
	Приложение 8. Инструкция по обработке персональных данных без использования средств автоматизации	31
	Приложение 9. Инструкция пользователя информационной системы персональных данных (ИСПДн)	33
	Приложение 10. Действия Пользователя информационной системы персональных данных и Ответственного за организацию обработки персональных данных при возникновении нештатных ситуаций	34
	Приложение 11. Порядок проведения инструктажа лиц, допущенных к работе с информационной системой персональных данных	35

## 1. Общие положения

**1.1.** Настоящее Положение является внутренним нормативным документом ПАО БАНК «СИАБ» (далее — Банк), определяющим меры по обеспечению информационной безопасности персональных данных сотрудников и клиентов Банка, а также иных лиц, персональные данные которых стали известны Банку в процессе осуществления им уставной деятельности.

Настоящее Положение вступает в действие с даты утверждения и является обязательным для соблюдения всеми подразделениями и сотрудниками Банка. Со дня начала действия настоящего Положения утрачивает действие «Положение о защите персональных данных», утвержденное 27.03.2018.

При изменениях законодательства Российской Федерации и нормативных правовых актов (далее - законодательство РФ) настоящее Положение подлежит актуализации, а до момента внесения в него изменений – применяется в части, не противоречащей законодательству РФ. При изменении Организационной структуры Банка Положение не требует внесения изменений, за исключением случаев, когда невозможно однозначно установить передачу полномочий и ответственности подразделений, обозначенных в настоящем Положении.

Изменения в настоящее Положение вносятся по инициативе Директора Департамента контроля информации, Вице-Президента по безопасности, Советника по информационной безопасности.

**1.2.** Положение разработано в соответствии с действующим законодательством РФ, в частности использованы:

– Федеральный закон от 02.12.1990 № 395-1 «О банках и банковской деятельности» (далее Закон № 395-1);

– Федеральный закон от 26.12.1995 № 208-ФЗ «Об акционерных обществах» (далее – Федеральный закон № 208-ФЗ);

– Федеральный закон от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» (далее – Федеральный закон № 115-ФЗ);

– Федеральный закон от 30.12.2004 № 218-ФЗ «О кредитных историях» (далее – Федеральный закон № 218-ФЗ);

– Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ);

– Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– Федеральный закон от 25.12.2008 № 273-ФЗ «О противодействии коррупции»;

– Федеральный закон от 27.07.2010 № 224-ФЗ «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации» (далее – Федеральный закон № 224-ФЗ);

– Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ (далее - Трудовой кодекс);

– Постановление Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» (далее - Постановление № 687);

– Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» (далее – Постановление № 1119);

– Постановление Правительства РФ от 15.06.2022 г. №1067 «О случаях и сроках использования биометрических персональных данных, размещенных физическими лицами в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение, биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным физического лица»;

– Приказ Федеральной службы по техническому и экспортному контролю (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»;

– Приказ Федеральной службы безопасности Российской Федерации (ФСБ России) от 10.07.2014 № 378 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации

Федерации требований к защите персональных данных для каждого из уровней защищенности» (далее - Приказ № 378);

– Положение Банка России от 20.07.2007 № 307-П «О порядке ведения учета и представления информации об аффилированных лицах кредитных организаций»;

– Положение Банка России от 15.10.2015 № 499-П «Об идентификации кредитными организациями клиентов, представителей клиента, выгодоприобретателей и бенефициарных владельцев в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»;

– Положение Банка России от 27.12.2017 № 625-П «О порядке согласования Банком России назначения (избрания) кандидатов на должности в финансовой организации, уведомления Банка России об избрании (прекращении полномочий), назначении (освобождении от должности) лиц, входящих в состав органов управления, иных должностных лиц в финансовых организациях, оценки соответствия квалификационным требованиям и (или) требованиям к деловой репутации лиц, входящих в состав органов управления, иных должностных лиц и учредителей (акционеров, участников) финансовых организаций, направления членом совета директоров (наблюдательного совета) финансовой организации информации в Банк России о голосовании (о непринятии участия в голосовании) против решения совета директоров (наблюдательного совета) финансовой организации, направления запроса о предоставлении Банком России информации и направления Банком России ответа о наличии (отсутствии) сведений в базах данных, предусмотренных статьями 75 и 76.7 Федерального закона от 10 июля 2002 года N 86-ФЗ «О Центральном банке Российской Федерации (Банке России)», а также о порядке ведения таких баз»;

Применяемые нормативные документы используются с учетом последующих изменений и дополнений.

**1.3.** Банк определяет порядок действий сотрудников при исполнении должностных обязанностей во внутренних нормативных документах, утвержденных уполномоченным органом управления Банка. Настоящее Положение разработано во взаимосвязи с иными внутренними нормативными документами Банка, в том числе:

«Политикой в отношении обработки персональных данных в ПАО БАНК «СИАБ»;

«Политикой информационной безопасности ПАО БАНК «СИАБ»;

«Инструкцией по обеспечению сохранности информации ограниченного доступа»;

«Порядком контроля доступа в помещения Банка»;

«Положением об организации видеонаблюдения в Банке»;

«Инструкцией о порядке обращения с носителями информации, содержащей персональные данные»;

«Регламентом поиска и подбора персонала»;

«Положением об управлении доступом к информационным системам»;

«Регламентом сбора, учета и изменения информации об аффилированных и связанных с Банком лицах»;

«Правилами внутреннего контроля по предотвращению, выявлению и пресечению неправомерного использования инсайдерской информации и (или) манипулирования рынком»;

«Правилами внутреннего контроля в целях противодействия легализации доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового уничтожения»;

«Инструкцией по организации архива»;

«Инструкцией по рассмотрению обращений субъектов персональных данных и их законных представителей»;

«Регламентом по работе с обращениями, поступающими в адрес Банка»;

«Порядком ведения электронного кадрового документооборота».

**1.4.** Используемые термины и определения:

**автоматизированная обработка персональных данных** - обработка персональных данных с помощью средств вычислительной техники. Обработка персональных данных не может быть признана осуществляемой с использованием средств автоматизации только на том основании, что персональные данные содержатся в информационной системе персональных данных либо были извлечены из нее;

**биометрические персональные данные** - сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются Банком (как оператором) для установления личности субъекта персональных данных;

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

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

**неавтоматизированная обработка персональных данных** - действия с персональными данными (использование, уточнение, распространение, уничтожение) в отношении каждого из субъектов персональных данных, осуществляемые при непосредственном участии человека;

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

**обеспечение защиты персональных данных** — систематический и документируемый процесс позволяющий исключить неправомерный или случайный доступ, уничтожение, изменение, блокирование, копирование, распространение или иные неправомерные действия при обработке персональных данных сотрудников, клиентов, контрагентов, используемых в деятельности Банка, выполняемый в рамках обеспечения информационной безопасности;

**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;

**персональные данные** (далее по тексту возможно использование термина ПДн) - любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных);

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

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

**Система JIRA** – программное обеспечение, используемое в качестве системы служебного документооборота, а также для организации и управления процессами сопровождения и решения задач по направлениям деятельности Банка;

**трансграничная передача персональных данных** - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу;

**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.

**Иные термины** применяются в определениях, установленных Федеральным законом № 152-ФЗ.

**1.5.** Подразделения и сотрудники Банка, ответственные за проведение процедур в соответствии с настоящим Положением:

Департамент контроля информации (далее – ДКИ) – структурное подразделение Банка, ответственное, в лице руководителя<sup>1</sup> ДКИ, за информационную безопасность, в частности, за организацию работы Банка по защите ПДн (обеспечению безопасности ПДн).

Департамент по работе с персоналом (далее – ДРП) – структурное подразделение Банка, о ответственное, в лице руководителя ДРП, за обработку ПДн сотрудников Банка, кандидатов на работу в Банке, их родственников, за хранение личных дел сотрудников.

Департамент информационных технологий (далее – ДИТ) - структурное подразделение Банка, ответственное, в лице руководителя ДИТ, за обеспечение функционирования информационной инфраструктуры Банка, в том числе, связанной с обработкой и защитой ПДн.

Корпоративный секретарь – сотрудник Банка, ответственный за обработку ПДн акционеров, членов Совета директоров, аффилированных и связанных с Банком лиц.

Уполномоченный сотрудник профессионального участника рынка ценных бумаг – сотрудник Банка, ответственный за обработку ПДн физических лиц, включенных в список инсайдеров.

Иные подразделения, сотрудники которых участвуют в обработке ПДн физических лиц - клиентов Банка, физических лиц, планирующих стать клиентами Банка (далее – потенциальный клиент), физических лиц – контрагентов Банка по договорам гражданско-правового характера.

---

<sup>1</sup> В рамках настоящего Положения под руководителем подразделения понимается должностное лицо, назначенное на соответствующую должность (директор, начальник, руководитель), а также его заместитель (если имеется) на период отсутствия такого руководителя или исполняющий обязанности такого руководителя в соответствии с приказом.

## **2. Цели обработки персональных данных**

**2.1.** Цели обработки Банком ПДн определены «Политикой в отношении обработки персональных данных в ПАО БАНК «СИАБ».

**2.2.** Банк обрабатывает ПДн клиентов, потенциальных клиентов, контрагентов в соответствии с требованиями законодательства РФ в целях оказания соответствующих финансовых услуг субъекту персональных данных, информирования, в том числе рекламного, субъекта персональных данных о банковских продуктах и продуктах партнеров, контроля качества обслуживания, выполнения договорных обязательств перед клиентами и контрагентами Банка, а также в целях выполнения требований, установленных законодательством РФ и нормативными актами Банка России.

**2.3.** Во исполнение норм трудового законодательства РФ Банк осуществляет сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение использование, передачу (предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных сотрудников Банка и кандидатов на работу.

В целях формирования и предоставления отчетности регулирующим органам в соответствии с требованиями законодательства РФ Банк осуществляет сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных акционеров и членов Совета директоров Банка, аффилированных и связанных с Банком лиц.

**2.4.** Банк не осуществляет обработку специальных категорий персональных данных, в т. ч. персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни.

**2.5.** Банк осуществляет обработку сведений о наличии / отсутствии судимости в отношении лиц, назначенных (в том числе временно) на соответствующие должности в Банке, установленные законодательством РФ, в целях подтверждения соответствия такого лица установленным законодательством РФ квалификационным требованиям и требованиям к деловой репутациям в течение всего периода исполнения соответствующих обязанностей.

**2.6.** Банк в установленных случаях осуществляет обработку биометрических персональных данных, порядок обработки описан в разделе 6 настоящего Положения.

**2.7.** Персональные данные получают непосредственно у субъекта персональных данных. В случае возникновения необходимости получения персональных данных субъекта ПДн у третьих лиц, субъект ПДн извещается о целях, предполагаемых источниках и способах получения путем подписания соответствующего письменного согласия.

**2.8.** Передача персональных данных третьей стороне не допускается без письменного согласия субъекта ПДн, за исключением случаев, установленных федеральными законами.

**2.9.** В процессе обработки Банком ПДн обеспечивается их конфиденциальность, за исключением случаев обезличивания персональных данных, а также общедоступных персональных данных.

**2.10.** Перечень персональных данных, в том числе биометрических персональных данных, обрабатываемых в Банке, определяется в соответствии с законодательством РФ и локальными актами Банка с учетом целей обработки персональных данных и в соответствии с уведомлением об обработке персональных данных, направленным Банком в Роскомнадзор<sup>2</sup>.

**2.11.** Полный перечень персональных данных, обрабатываемых в Банке, с указанием категорий субъектов персональных данных, представлен в приложении 1 к настоящему Положению.

**2.12.** Общие и частные цели обработки персональных данных в Банке представлены в приложении 2 к настоящему Положению.

## **3. Сбор и дальнейшая обработка персональных данных**

**3.1.** Сотрудник Банка при получении от клиентов информации с ПДн проверяет достоверность сведений, сверяя данные, предоставленные субъектом ПДн, с имеющимися у субъекта ПДн документами.

**3.2.** Персональные данные субъекта ПДн предоставляются вместе с обязательным письменным согласием субъекта ПДн на обработку его персональных данных, включая, при необходимости, согласие на передачу персональных данных третьим лицам. Сотрудники Банка, осуществляющие подготовку типовых форм бланков, заявлений, анкет и т.д., в установленных законодательством случаях включают в такие документы утвержденный настоящим Положением

<sup>2</sup> Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций

текст согласия на обработку данных (форма приведена в приложении 4 к настоящему Положению).

**3.3.** Правовое основание обработки персональных данных, обрабатываемых в Банке, приведено в приложении 3 к настоящему Положению.

**3.4.** Полученные персональные данные субъекта ПДн для дальнейшей обработки:

- хранятся на бумажном носителе;
- заносятся в автоматизированные банковские системы (информационные системы);
- передаются контрагентам Банка при осуществлении расчетного обслуживания, переводов денежных средств, деятельности на рынке ценных бумаг на основании действующих договоров (соглашений);

- передаются уполномоченным государственным органам в случаях, установленных законодательством РФ.

**3.5.** Передача персональных данных третьим лицам на основании договоров (соглашений) осуществляется при условии наличия в договорах (соглашениях) положений об обеспечении третьим лицом конфиденциальности получаемых персональных данных и безопасности персональных данных при их обработке.

**3.6.** Обработка персональных данных прекращается Банком по требованию субъекта ПДн, либо по достижении целей их обработки, либо при утрате необходимости в их достижении.

**3.7.** Обработка персональных данных прекращается Банком по требованию субъекта ПДн, либо по достижении целей их обработки, либо при утрате необходимости в их достижении.

**3.8.** Сроки архивного хранения документов, содержащих персональные данные, приведены в приложении 6 к настоящему Положению.

**3.9.** в случае автоматизированной обработки уничтожение информации (персональных данных) с материальных носителей персональных данных и уничтожение самих носителей производится в соответствии с «Порядком работы с материальными носителями персональных данных».

#### **4. Основные меры обеспечения защиты персональных данных**

**4.1.** Для обеспечения безопасности при обработке и защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения, а также от иных неправомерных действий при обработке персональных данных Банком используются организационные и технические меры:

- определение требований к сотрудникам, имеющих доступ к персональным данным, посредством включения в должностные соответствующих дополнений (пунктов);

- определение угроз безопасности персональных данных и разработка защитных мер;

- учет носителей персональных данных и средств их защиты;

- недопущение нарушения функционирования средств обработки и обеспечение восстановления персональных данных, модифицированных или уничтоженных;

- постоянный контроль за обеспечением уровня защищенности и технические меры:

- шифровальные (криптографические) средства;

- средства предотвращения несанкционированного доступа и (или) передачи;

- средства защиты помещений, исключающие неконтролируемое проникновение или пребывание в них посторонних;

- ведение в информационных системах электронных журналов обращений и получения доступа.

- обнаружение фактов несанкционированного доступа к персональным данным и принятие 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;

- восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

- разработка 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;

- контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

**4.2.** Порядок формирования состава средств защиты персональных данных определяется приложением 5 к настоящему Положению.

#### **5. Порядок и условия обработки персональных данных сотрудников**

**5.1.** Сбор ПДн сотрудников осуществляется уполномоченными Банком лицами в общем порядке в соответствии с настоящим Положением.

**5.2.** Департамент по работе с персоналом, осуществляющий подбор персонала, получает ПДн кандидата для трудоустройства на вакантную должность (далее – кандидат) в формате резюме, составленного кандидатом в свободной форме, по электронной почте или через специализированные ресурсы в сети Интернет, либо на бумажном носителе.

**5.3.** Для подтверждения факта направления резюме самим кандидатом и последующего рассмотрения возможности его трудоустройства в Банке сотрудники ДРП приглашают кандидата, удовлетворяющего установленным требованиям к вакантной должности, на личную встречу с уполномоченными сотрудниками Банка (собеседование).

**5.4.** При поступлении в адрес Банка по электронной почте резюме, составленного в произвольной форме, при которой однозначно определить физическое лицо, его направившее, не представляется возможным, данное резюме подлежит уничтожению в день поступления. Сведения о получении такого электронного письма (содержащего резюме), а также факте уничтожения учитываются (хранятся) в журналах корпоративного почтового сервера.

**5.5.** Согласие на обработку ПДн кандидата содержится в последнем разделе анкеты. Сбор и последующая обработка персональных данных кандидата, указываемых в анкете, в том числе в целях проверки добросовестности кандидата и принятия решения о заключении трудового договора с кандидатом, осуществляется на основании подписанной им анкеты.

**5.6.** Ответственность за сбор согласий кандидатов, их хранение и своевременное уничтожение возлагается на ДРП.

**5.7.** Кандидат, в отношении которого Банком принято решение о приеме на работу, предоставляет в ДРП, в котором будет храниться личное дело сотрудника, документы для заключения трудового договора.

**5.8.** В общих случаях для обработки ПДн сотрудников не требуется получения согласия, так как обработка осуществляется Банком для заключения и исполнения трудового договора, а также для выполнения возложенных законодательством РФ на Банк функций, полномочий и обязанностей.

**5.9.** Банк, при наличии производственной необходимости, может дополнительно получать согласия сотрудников на передачу их ПДн третьим лицам (страховые компании, учебные заведения и т.п.).

**5.10.** Согласия на обработку ПДн оформляются в письменном виде с соблюдением требований к их содержанию, установленных Федеральным законом № 152-ФЗ.

**5.11.** Ответственность за получение согласий сотрудников на обработку ПДн и их хранение возлагается на ДРП. Форма согласия на обработку персональных данных установлена «Порядком ведения электронного кадрового документооборота».

**5.12.** В случае если ПДн кандидата или сотрудника возможно получить только у третьей стороны, ДРП направляет кандидату или сотруднику соответствующее уведомление, в котором указываются следующие сведения:

- цели получения ПДн;
- предполагаемые источники и способы получения ПДн;
- характер подлежащих получению ПДн;
- запрос письменного согласия на получение ПДн, сроки предоставления согласия и последствия отказа его предоставить.

**5.13.** Кандидат или сотрудник, получивший указанное уведомление, должен предоставить в ДРП письменное согласие либо письменный отказ в течение установленного в уведомлении срока.

**5.14.** Запись, систематизация и накопление полученных ПДн кандидатов и сотрудников осуществляется уполномоченными Банком лицами в общем порядке в соответствии с настоящим Положением.

**5.15.** Хранение ПДн кандидатов и сотрудников осуществляется сотрудниками ДРП в общем порядке в соответствии с настоящим Положением.

Хранение ПДн кандидатов и сотрудников на бумажных носителях осуществляется в папках и делах, сформированных в зависимости от содержащихся в них ПДн и целей обработки этих ПДн, в специально отведенных для этого местах в помещениях, занимаемых сотрудниками Банка, допущенными к работе с ПДн, в частности:

- ПДн на бумажных носителях, составляющие личное дело сотрудника, хранятся в папках в ДРП в специальном металлическом шкафу, закрываемом на ключ, обеспечивающем защиту от несанкционированного доступа;
- личные карточки сотрудников и трудовые книжки сотрудников (в случае их ведения на бумажном носителе) хранятся в сейфовом шкафу в помещении ДРП;
- документы, необходимые для расчетов по оплате труда, содержащие ПДн сотрудников, хранятся в Отделе внутрибанковских операций Департамента бухгалтерского учета и отчетности в шкафах, закрываемых на ключ, обеспечивающих защиту от несанкционированного доступа.



Ответственность за сохранность ПДн кандидатов и сотрудников на бумажных носителях возложена на сотрудников подразделений, осуществляющих формирование и использование таких документов в рамках выполнения своих функциональных обязанностей.

Хранение ПДн кандидатов и сотрудников в электронном виде осуществляется в базах данных автоматизированных систем, доступ к которым ограничен.

Ответственность за организацию защиты ПДн кандидатов и сотрудников в электронном виде (применение необходимых организационных и технических мер защиты) возложена на ДКИ и Департамент информационных технологий (ДИТ) в соответствии с их компетенцией (функциями).

**5.16.** Использование, извлечение и уточнение ПДн кандидатов и сотрудников осуществляется сотрудниками ДРП в общем порядке в соответствии с настоящим Положением.

ПДн кандидатов и сотрудников используются исключительно для целей, установленных в настоящем Положении.

ДРП вправе передавать ПДн сотрудника в иные структурные подразделения Банка для обеспечения необходимости исполнения сотрудниками соответствующих структурных подразделений своих функциональных обязанностей по запросу. Указанный запрос должен быть согласован сотрудником, ответственным за организацию обработки ПДн, назначенных Приказом по Банку из числа сотрудников ДКИ.

При передаче ПДн сотрудника руководитель ДРП предупреждает лиц, получающих данную информацию, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены.

**5.17.** Передача ПДн кандидатов и сотрудников осуществляется сотрудниками ДРП в общем порядке в соответствии с настоящим Положением.

Информация, относящаяся к ПДн сотрудника, может быть предоставлена государственным органам в порядке, установленном законодательством РФ.

В соответствии со статьей 88 Трудового кодекса при передаче персональных данных сотрудника уполномоченные Банком лица должны соблюдать следующие требования:

- не сообщать ПДн сотрудника третьей стороне без письменного согласия сотрудника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью сотрудника, а также в случаях, установленных Трудовым кодексом и иными федеральными законами;

- не сообщать ПДн сотрудника в коммерческих целях без его письменного согласия;

- предупредить лиц, получающих ПДн сотрудника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено.

**5.18.** Блокирование ПДн кандидатов и сотрудников осуществляется уполномоченными Банком лицами в общем порядке в соответствии с настоящим Положением.

**5.19.** Удаление, уничтожение и обезличивание ПДн кандидатов и сотрудников осуществляется уполномоченными Банком лицами в общем порядке в соответствии с настоящим Положением.

## **6. Порядок и условия обработки биометрических персональных данных**

**6.1.** Обработка биометрических персональных данных осуществляется Банком в соответствии с требованиями к защите биометрических персональных данных, установленными в соответствии со статьей 19 Федерального закона № 152-ФЗ.

**6.2.** Здания и помещения Банка оборудованы телевизионной системой наблюдения и регистрации (далее - ТСНР), осуществляющей видеонаблюдение, непрерывную видеорегистрацию и хранение в цифровом виде видеоинформации о действиях сотрудников Банка и посетителей. Целью видеонаблюдения являются обеспечение безопасных условий работы сотрудников Банка, обеспечение защиты информации в платежной системе Банка России, обеспечение сохранности наличных денег, материальных ценностей, соблюдение прав клиентов, обеспечение их безопасности, мониторинг (предупреждение) возникновения чрезвычайных и нестандартных ситуаций и обеспечение объективности расследования в случаях их возникновения.

**6.3.** ТСНР является открытой, не направлена на сбор информации о конкретном физическом лице и входит в состав единой технической системы безопасности Банка совместно с охранно-пожарной сигнализацией, системой контроля и управления доступом (далее - СКУД). Об осуществлении видеонаблюдения на объектах Банка сотрудники оповещаются путем ознакомления с Правилами внутреннего трудового распорядка.

**6.4.** Кассовые работники Банка дополнительно оповещаются об оборудовании видеорекамерами, осуществляющими непрерывную видеозапись, их рабочих мест в операционных кассах, кассовых узлах, сейфовых комнатах, хранилищах ценностей в целях осуществления контроля.

**6.5.** Клиенты оповещаются о наличии системы видеонаблюдения надписями и символами установленного типа на видных местах. В Банке запрещено использование устройств для негласного получения информации (скрытых камер).

**6.6.** При проходе на территорию Банка идентификация и (или) аутентификация с использованием биометрических данных физических лиц посредством использования информационных систем, обеспечивающих функционирование пропускных пунктов, не осуществляется.

**6.7.** Использование и хранение биометрических персональных данных вне информационных систем персональных данных осуществляется на материальных носителях информации и с применением технологии ее хранения, которые обеспечивают защиту этих данных от неправомерного или случайного доступа к ним, их уничтожения, изменения, блокирования, копирования, предоставления, распространения.

**6.8.** Технология хранения биометрических персональных данных вне информационных систем персональных данных обеспечивает:

– доступ к информации, содержащейся на материальном носителе, для уполномоченных лиц;

– применение средств электронной подписи или иных информационных технологий, позволяющих сохранить целостность и неизменность биометрических персональных данных, записанных на материальный носитель;

– обеспечение наличия письменного согласия субъекта персональных данных на обработку его биометрических персональных данных или наличия иных оснований обработки персональных данных, установленных законодательством РФ в сфере отношений, связанных с обработкой персональных данных.

**6.9.** При хранении биометрических персональных данных вне информационных систем персональных данных обеспечивается регистрация фактов несанкционированной повторной и дополнительной записи информации после ее извлечения из информационной системы персональных данных.

## **7. Порядок обработки обращений субъектов персональных данных**

Банк осуществляет прием и рассмотрение обращений субъектов персональных данных или их законных представителей, касающихся обработки персональных данных субъекта персональных данных, ознакомления с его персональными данными, уточнения, уничтожения, блокирования его персональных данных, отзыва согласия на обработку его персональных данных, устранения неправомерных действий с его персональными данными, в соответствии с порядком и сроками, установленными Федеральным законом № 152-ФЗ и «Инструкцией по рассмотрению обращений субъектов персональных данных и их законных представителей».

## **8. Порядок доступа к персональным данным, передача уполномоченным государственным органам**

**8.1.** Доступ к персональным данным сотрудников Банка предоставляется сотрудникам ДРП на постоянной основе, а также руководителям подразделений Банка по отдельным заявкам.

**8.2.** Доступ к персональным данным клиентов предоставляется сотрудникам Банка в соответствии перечнем должностей, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным, утверждаемым приказом по Банку (далее – Перечень). Матрица соответствия ролей (должностей) сотрудников Банка и уровней доступа к персональным данным ведется в ДКИ в электронном виде.

Перечень должностей пересматривается в случае внесения изменений в организационно-штатную структуру Банка, но не реже одного раза в год.

Подразделением, ответственным за актуализацию Перечня, является ДКИ.

**8.3.** Перед предоставлением доступа к персональным данным сотрудник в обязательном порядке проходит инструктаж по обеспечению защиты персональных данных при их обработке и дает письменное обязательство по выполнению необходимых мер защиты.

**8.4.** Внутренний доступ.

Право доступа к персональным данным клиентов Банка имеют:

– руководство Банка: Президент-Председатель Правления (лицо, его замещающее), Главный бухгалтер (лицо, его замещающее);

– Служба внутреннего аудита: при проведении проверок;

– сотрудники, получившие доступ в установленном порядке для выполнения должностных обязанностей или заданий.

**8.5.** Внешний доступ.

К числу лиц, имеющих доступ к персональным данным клиентов Банка в силу положений законодательства РФ, относятся представители следующих государственных органов:

- Роскомнадзор - при осуществлении проверок выполнения требований законодательства РФ в области защиты персональных данных;
- Банк России - при осуществлении надзорной деятельности;
- Федеральная налоговая служба;
- правоохранительные органы;
- иные уполномоченные органы в пределах своей компетенции.

**8.6.** В Банке ведется учет помещений, в которых обрабатываются персональные данные.

8.6.1. К помещениям, в которых ведется обработка персональных данных, относятся помещения, в которых происходит обработка персональных данных, как с использованием средств автоматизации, так и без таковых, а также хранятся резервные копии персональных данных и ключевые документы к ним.

8.6.2. Доступ в помещения Банка, в которых ведется обработка персональных данных, осуществляется в соответствии со Списком доступа, утверждаемым Вице-президентом по безопасности.

8.6.3. Для помещений, в которых ведется обработка персональных данных, организуется режим обеспечения безопасности, при котором обеспечивается сохранность носителей информации, содержащих персональные данные, а также исключается возможность неконтролируемого проникновения и пребывания в этих помещениях посторонних лиц. Данный режим обеспечивается в том числе:

запираанием помещения на ключ, в том числе при выходе из него в рабочее время; закрытием металлических шкафов и сейфов, где хранятся носители информации, содержащие персональные данные, во время отсутствия в помещении сотрудников, замещающих должности, предусмотренные Перечнем.

8.6.4. Шкафы, ящики и сейфы, предназначенные для хранения материальных носителей персональных данных и конфиденциальной информации, запираются после завершения их использования и опечатываются по окончании рабочего дня (если режим использования мест хранения, предусмотренный внутренними документами Банка, предполагает их обязательное опечатывание). Оттиски печатей, наносимые на приспособления для опечатывания входных и запасных дверей (при их наличии), запираемых шкафов, ящиков и сейфов, должны иметь четкий рисунок. Для удобства проверки качества опечатывания дверей помещений оттиски печатей необходимо наносить с таким расчетом, чтобы цифровая и буквенная надписи оттиска располагались горизонтально.

8.6.5. Доступ посторонних лиц в помещения, в которых ведется обработка персональных данных, возможен только ввиду служебной необходимости.

На момент присутствия посторонних лиц в помещении, в котором ведется обработка персональных данных, должны быть приняты меры по недопущению ознакомления посторонних лиц с персональными данными.

8.6.6. Ответственность за соблюдение порядка доступа в помещения, в которых ведется обработка персональных данных, возлагается на сотрудника, на которого Приказом по Банку возложены функции ответственного за организацию обработки ПДн.

8.6.7. Список помещений, в которых ведется обработка персональных данных, включается в «Перечень категоризованных помещений Банка (по форме приложения 2 к «Порядку контроля доступа в помещения Банка»), который составляется, поддерживается в актуальном состоянии сотрудниками Информационно-аналитического департамента (далее – ИАД) по согласованию с ДКИ, утверждается Вице-Президентом по безопасности.

8.6.8. Сотрудники, назначенные ответственными за соответствующие помещения, информируют сотрудника ДКИ, ответственного за организацию обработки ПДн, об изменениях в составе помещений не позднее 3 рабочих дней со дня таких изменений.

## **9. Обязанности сотрудников**

**9.1.** В целях обеспечения актуальности обрабатываемых ПДн в случае изменений ПДн сотрудник обязан в течение семи рабочих дней сообщить в ДРП сведения:

- об изменении адреса регистрации по месту жительства, адреса регистрации по месту пребывания, адреса фактического места жительства, номера телефона;
- о замене паспорта;
- об изменении гражданского состояния (перемене своего имени, включающего в себя фамилию, собственно имя и (или) отчество, семейного положения, рождении детей и т.д.);
- об изменении сведений о воинском учете;
- об окончании учебных заведений.

**9.2.** Сотрудники Банка, выполняющие обработку персональных данных клиентов Банка, обязаны соблюдать требования по защите персональных данных клиентов Банка при их обработке, а именно:

9.2.1. Знать и руководствоваться в работе следующими внутренними документами Банка:

- «Порядок обеспечения непрерывности и реагировании на инцидент при эксплуатации технических средств и программного обеспечения, баз данных и средств защиты информации ИСПДн» (приложение 7 к настоящему Положению);
- «Инструкция по обработке персональных данных без использования средств автоматизации» (приложение 8 к настоящему Положению);
- «Инструкция пользователя Информационной системы персональных данных (ИСПДн)» (приложение 9 к настоящему Положению);
- «Действия Пользователя Информационной системы персональных данных и Ответственного за организацию обработки персональных данных при возникновении нештатных ситуаций» (приложение 10 к настоящему Положению);

9.2.2. Пройти вводный инструктаж перед началом обработки персональных данных в соответствии с «Порядком проведения инструктажа лиц, допущенных к работе с Информационной системой персональных данных» (приложение 11 к настоящему Положению).

## **10. Права сотрудников в целях обеспечения защиты персональных данных, хранящихся в Банке**

**10.1.** В целях обеспечения защиты персональных данных, хранящихся в Банке, сотрудники имеют право:

- на свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные сотрудника, за исключением случаев, предусмотренных федеральным законом. Получение указанной информации сотрудниками в отношении своих персональных данных возможно при личном обращении сотрудника в ДРП или Департамент бухгалтерского учета и отчетности. Выписки из личного дела сотрудника, приказов и иных документов, связанных с работой, выдаются сотруднику на основании его письменного заявления в течение трех дней с момента подачи заявления;

- определение своих представителей для защиты своих персональных данных;

- доступ к относящимся к ним медицинским данным с помощью медицинского специалиста по их выбору;

- требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований Трудового кодекса. При обнаружении неверных, неполных, а равно полученных с нарушением Трудового кодекса персональных данных сотрудник должен обратиться с заявлением на имя Президента-Председателя Правления Банка об исправлении (исключении) подобных сведений. При отказе Банка исключить или исправить персональные данные сотрудника он имеет право заявить в письменной форме о своем несогласии с соответствующим обоснованием такого несогласия.

**10.2.** Персональные данные оценочного характера сотрудник имеет право дополнить заявлением, выражающим его собственную точку зрения;

- требование об извещении Банком всех лиц, которым ранее были сообщены неверные или неполные персональные данные работника, обо всех произведенных в них исключениях, исправлениях или дополнениях;

- обжалование в суд любых неправомерных действий или бездействия Банка при обработке и защите его персональных данных.

## **11. Организация контроля выполнения требований по защите персональных данных**

**11.1.** Контроль выполнения требований по защите персональных данных осуществляется в целях оценки фактического состояния защиты персональных данных, выявления недостатков и нарушений, установления причин недостатков и нарушений, выработки мер для их устранения, исключения повторений и повышения уровня защиты в целом. Порядок осуществления контроля определяется руководителем ДКИ, с учетом приведенных ниже требований.

**11.2.** Контролю подлежат все:

- структурные подразделения (помещения, сотрудники), обрабатывающие персональные данные;

- информационные системы, содержащие персональные данные;

- носители информации, на которых хранятся персональные данные;

– коммуникационные каналы, по которым передается информация, содержащая персональные данные.

**11.3.** В состав мероприятий по контролю могут быть включены все или некоторые (при проведении выборочного контроля) мероприятия:

- проверка полноты, качества, актуальности утвержденных внутренних нормативных и распорядительных документов, регламентирующих обработку и обеспечение безопасности ПДн;
- контроль выполнения требований по режиму доступа в помещения и к АРМ, где ведется обработка ПДн;
- проверка порядка использования средств защиты информации и средств криптографической защиты информации ПДн;
- проверка выполнения требований действующих внутренних нормативных документов по защите персональных данных;
- проверка и выявления изменений в режиме обработки ПДн;
- анализ и пересмотр имеющихся угроз безопасности ПДн, выявление новых угроз;
- проверка актуальности сведений в Реестре операторов персональных данных Роскомнадзора.

Ответственный за организацию обработки персональных данных либо специально созданная приказом по Банку комиссия по выполнению требований Федерального закона № 152-ФЗ проводят контроль непосредственно на месте обработки персональных данных, опрашивают сотрудников, осуществляющих обработку персональных данных, осматривают рабочие места. Сотрудники обязаны по запросу контролирующих предъявить все материалы и документы, числящиеся за ними, давать устные или письменные объяснения по существу заданных вопросов.

По результатам проверки составляется акт контроля выполнения требований законодательства РФ в области персональных данных.

## **12. Ответственность за нарушение требований по защите персональных данных**

Лица, виновные в нарушении требований законодательства РФ, регулирующих получение, обработку и защиту персональных данных субъекта персональных данных, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

## Перечень персональных данных, обрабатываемых в Банке

№ п/п	Группа персональных данных	Содержание сведений	Категория ПДн <sup>3</sup>
<b>1</b>	<b>Персональные данные кандидатов для трудоустройства на вакантную должность</b>		
1.1	Контактные данные	– Ф.И.О.; – номер телефона; – e-mail	И
1.2	Сведения о дате и месте рождения	– Ф.И.О.; – прежняя фамилия и дата смены (в случае смены фамилии); – дата рождения; – место рождения	И
1.3	Сведения о гражданстве	– Ф.И.О.; – гражданство	И
1.4	Сведения о семейном положении	– Ф.И.О.; – семейное положение	И
1.5	Сведения о месте жительства	– Ф.И.О.; – адрес регистрации по месту жительства; – адрес фактического места жительства; – адрес регистрации по месту временного пребывания (адрес, дата регистрации, наименование органа, осуществившего регистрацию, срок регистрации)	И
1.6	Паспортные данные или данные иного документа, удостоверяющего личность	– Ф.И.О.; – наименование документа, удостоверяющего личность; – серия и номер документа; – дата выдачи документа; – наименование органа, выдавшего документ; – код подразделения	И
1.7	Сведения об образовании	– Ф.И.О.; – наименование оконченного учебного заведения; – факультет; – форма обучения; – период обучения; – специальность; – квалификация	И
1.8	Сведения о дополнительном образовании	– Ф.И.О.; – наименование оконченного учебного заведения; – период обучения; – название курса, тренинга – данные документа, подтверждающего окончание курса	И
1.9	Сведения о дополнительных навыках	– Ф.И.О.; – уровень владения программными приложениями; – уровень владения иностранными языками; – достижения в профессиональной деятельности	И
1.10	Сведения о воинской обязанности	– Ф.И.О.; – отношение к воинской обязанности	И
1.11	Сведения о привлечении к ответственности в судебном порядке	– Ф.И.О.; – наличие/отсутствие случаев привлечения к ответственности в судебном порядке	С

<sup>3</sup> Специальные категории ПДн (С) / Биометрические ПДн (Б) / Общедоступные ПДн (О) / Иные ПДн (И)

№ п/п	Группа персональных данных	Содержание сведений	Категория ПДн <sup>3</sup>
1.12	Сведения о трудовой деятельности	<ul style="list-style-type: none"> <li>– Ф.И.О.;</li> <li>– наименование работодателя, адрес;</li> <li>– период работы;</li> <li>– должность;</li> <li>– причина увольнения</li> </ul>	И
<b>2</b>	<b>Персональные данные сотрудников</b>		
2.1	Паспортные данные или данные иного документа, удостоверяющего личность	<ul style="list-style-type: none"> <li>– Ф.И.О.;</li> <li>– наименование документа, удостоверяющего личность;</li> <li>– серия и номер документа;</li> <li>– дата выдачи документа;</li> <li>– срок действия (для заграничного паспорта);</li> <li>– наименование органа, выдавшего документ;</li> <li>– код подразделения</li> </ul>	И
2.2	Сведения о дате и месте рождения, пол	<ul style="list-style-type: none"> <li>– Ф.И.О.;</li> <li>– дата рождения;</li> <li>– место рождения;</li> <li>– пол</li> </ul>	И
2.3	Сведения о месте жительства	<ul style="list-style-type: none"> <li>– Ф.И.О.;</li> <li>– адрес регистрации по месту жительства;</li> <li>– адрес фактического места жительства;</li> <li>– адрес регистрации по месту временного пребывания (адрес, дата регистрации, наименование органа, осуществившего регистрацию, срок регистрации)</li> </ul>	И
2.4	Контактные данные	<ul style="list-style-type: none"> <li>– Ф.И.О.;</li> <li>– номер телефона (мобильный, домашний, рабочий);</li> <li>– e-mail</li> </ul>	И
2.5	Сведения о гражданстве	<ul style="list-style-type: none"> <li>– Ф.И.О.;</li> <li>– гражданство</li> </ul>	И
2.6	Сведения об образовании	<ul style="list-style-type: none"> <li>– Ф.И.О.;</li> <li>– наименование оконченного учебного заведения;</li> <li>– факультет;</li> <li>– форма обучения;</li> <li>– серия и номер документа об образовании;</li> <li>– период обучения;</li> <li>– специальность;</li> <li>– квалификация;</li> <li>– профессия</li> </ul>	И
2.7	Сведения о дополнительном образовании	<ul style="list-style-type: none"> <li>– Ф.И.О.;</li> <li>– наименование оконченного учебного заведения;</li> <li>– период обучения;</li> <li>– название курса, тренинга;</li> <li>– данные документа, подтверждающего окончание курса</li> </ul>	И
2.8	Сведения о трудовой деятельности	<ul style="list-style-type: none"> <li>– Ф.И.О.;</li> <li>– наименование работодателя, адрес;</li> <li>– период работы;</li> <li>– должность;</li> <li>– причина увольнения</li> </ul>	И
2.9	Сведения о трудовом стаже	<ul style="list-style-type: none"> <li>– Ф.И.О.;</li> <li>– общий стаж работы;</li> <li>– стаж, дающий право на надбавку за выслугу лет</li> </ul>	И
2.10	Сведения о воинском учете	<ul style="list-style-type: none"> <li>– Ф.И.О.;</li> <li>– отношение к воинской обязанности;</li> <li>– воинское звание</li> </ul>	И

№ п/п	Группа персональных данных	Содержание сведений	Категория ПДн <sup>3</sup>
2.11	Данные военного билета	<ul style="list-style-type: none"> <li>- Ф.И.О.;</li> <li>- серия и номер военного билета;</li> <li>- дата выдачи военного билета;</li> <li>- наименование военного комиссариата, выдавшего военный билет</li> </ul>	И
2.12	Данные свидетельства государственного пенсионного страхования	<ul style="list-style-type: none"> <li>- Ф.И.О.;</li> <li>- номер свидетельства ОПС (СНИЛС)</li> </ul>	И
2.13	Данные свидетельства о постановке на учет в налоговом органе	<ul style="list-style-type: none"> <li>- Ф.И.О.;</li> <li>- дата постановки на учет в налоговом органе;</li> <li>- ИНН;</li> <li>- наименование и код налогового органа</li> </ul>	И
2.14	Данные водительского удостоверения	<ul style="list-style-type: none"> <li>- Ф.И.О.;</li> <li>- серия и номер водительского удостоверения;</li> <li>- кем и когда выдано водительское удостоверение;</li> <li>- стаж вождения</li> </ul>	И
2.15	Сведения о семейном положении	<ul style="list-style-type: none"> <li>- Ф.И.О.;</li> <li>- семейное положение</li> </ul>	И
2.16	Сведения о браке	<ul style="list-style-type: none"> <li>- Ф.И.О.;</li> <li>- Ф.И.О. супруга/супруги;</li> <li>- дата и место заключения брака;</li> <li>- дата расторжения брака</li> </ul>	И
2.17	Сведения о детях	<ul style="list-style-type: none"> <li>- Ф.И.О.;</li> <li>- Ф.И.О. детей;</li> <li>- пол;</li> <li>- дата и место рождения детей</li> </ul>	И
2.18	Сведения о трудовом договоре	<ul style="list-style-type: none"> <li>- Ф.И.О.;</li> <li>- дата заключения договора;</li> <li>- номер договора;</li> <li>- срок действия договора</li> </ul>	И
2.19	Сведения об условиях трудоустройства	<ul style="list-style-type: none"> <li>- Ф.И.О.;</li> <li>- срок испытания при приеме на работу;</li> <li>- тип работы (основная работа, по совместительству, для замещения временно отсутствующего сотрудника и т.п.)</li> </ul>	И
2.20	Сведения о должности	<ul style="list-style-type: none"> <li>- Ф.И.О.;</li> <li>- структурное подразделение;</li> <li>- должность</li> </ul>	И
2.21	Данные пропуска в здание и помещения Банка	<ul style="list-style-type: none"> <li>- Ф.И.О.;</li> <li>- номер пропуска;</li> <li>- номер служебного удостоверения</li> </ul>	И
2.22	Сведения о заработной плате	<ul style="list-style-type: none"> <li>- Ф.И.О.;</li> <li>- тарифная ставка (должностной оклад);</li> <li>- размер надбавки</li> </ul>	И
2.23	Сведения о социальных льготах	<ul style="list-style-type: none"> <li>- Ф.И.О.;</li> <li>- наименование социальной льготы;</li> <li>- данные подтверждающего документа</li> </ul>	И
2.24	Сведения об отпуске	<ul style="list-style-type: none"> <li>- Ф.И.О.;</li> <li>- вид отпуска;</li> <li>- период отпуска</li> </ul>	И
2.25	Сведения о смене анкетных данных	<ul style="list-style-type: none"> <li>- Ф.И.О.;</li> <li>- дата внесения изменений;</li> <li>- причина внесения изменений</li> </ul>	И
2.26	Сведения о временной нетрудоспособности	<ul style="list-style-type: none"> <li>- Ф.И.О.;</li> <li>- причина временной нетрудоспособности;</li> <li>- срок временной нетрудоспособности</li> </ul>	И
2.27	Сведения о прекращении трудового договора	<ul style="list-style-type: none"> <li>- Ф.И.О.;</li> <li>- дата прекращения трудового договора;</li> <li>- основание прекращения трудового договора</li> </ul>	И



№ п/п	Группа персональных данных	Содержание сведений	Категория ПДн <sup>3</sup>
2.28	Банковские реквизиты	<ul style="list-style-type: none"> <li>- Ф.И.О.;</li> <li>- реквизиты банка;</li> <li>- номер текущего счета</li> </ul>	И
2.29	Сведения о банковской карте	<ul style="list-style-type: none"> <li>- Ф.И.О.;</li> <li>- номер банковской карты;</li> <li>- срок действия;</li> <li>- номер банковского счета;</li> <li>- дата выпуска;</li> <li>- лимит;</li> <li>- кодовое слово</li> </ul>	И
2.30	Сведения о начислении заработной платы	<ul style="list-style-type: none"> <li>- Ф.И.О.</li> <li>- сумма к начислению</li> </ul>	И
2.31	Сведения о сумме отпускных	<ul style="list-style-type: none"> <li>- Ф.И.О.</li> <li>- размер суммы отпускных</li> </ul>	И
2.32	Сведения о размере компенсационных выплат	<ul style="list-style-type: none"> <li>- Ф.И.О.</li> <li>- размер компенсационных выплат</li> </ul>	И
2.33	Сведения о размере пособия по временной нетрудоспособности	<ul style="list-style-type: none"> <li>- Ф.И.О.;</li> <li>- размер пособия по временной нетрудоспособности</li> </ul>	И
2.34	Сведения о размере выплаты при увольнении сотрудника	<ul style="list-style-type: none"> <li>- Ф.И.О.;</li> <li>- сумма к выплате при увольнении</li> </ul>	И
2.35	Сведения о начисленных/удержанных средствах	<ul style="list-style-type: none"> <li>- Ф.И.О.;</li> <li>- сумма к начислению/удержанию</li> </ul>	И
2.36	Сведения об отчислениях в Фонд пенсионного и социального страхования Российской Федерации	<ul style="list-style-type: none"> <li>- Ф.И.О.;</li> <li>- страховой стаж;</li> <li>- размер страховых взносов</li> </ul>	И
2.37	Сведения об исчисленных, удержанных и перечисленных в бюджетную систему Российской Федерации налогах	<ul style="list-style-type: none"> <li>- Ф.И.О.;</li> <li>- размер налоговых перечислений</li> </ul>	И
2.38	Сведения о кредитных обязательствах	<ul style="list-style-type: none"> <li>- Ф.И.О.</li> <li>- наименование банка, микрофинансовой организации, кредитного кооператива;</li> <li>- сумма кредита, займа;</li> <li>- наличие просроченных платежей;</li> <li>- сумма задолженности</li> </ul>	И
2.39	Сведения о привлечении к ответственности в судебном порядке	<ul style="list-style-type: none"> <li>- Ф.И.О.;</li> <li>- наличие/отсутствие случаев привлечения к ответственности в судебном порядке</li> </ul>	С
2.40	Сведения о наличии алиментных обязательств	<ul style="list-style-type: none"> <li>- Ф.И.О.;</li> <li>- размер взыскиваемых алиментов;</li> <li>- срок алиментных обязательств;</li> <li>- данные документа, подтверждающего наличие алиментных обязательств (вид, номер, дата выдачи)</li> </ul>	И

№ п/п	Группа персональных данных	Содержание сведений	Категория ПДн <sup>3</sup>
2.41	Сведения о наличии инвалидности	<ul style="list-style-type: none"> <li>– Ф.И.О.;</li> <li>– группа инвалидности;</li> <li>– дата установления инвалидности;</li> <li>– срок инвалидности;</li> <li>– данные документа, подтверждающего наличие инвалидности (вид, номер, дата выдачи);</li> <li>– степень ограничения способности к трудовой деятельности;</li> <li>– причина инвалидности;</li> <li>– перечень и степень ограничений основных категорий жизнедеятельности;</li> <li>– мероприятия медицинской реабилитации и срок их проведения;</li> <li>– мероприятия профессиональной реабилитации и срок их проведения;</li> <li>– мероприятия социальной реабилитации и срок их проведения;</li> <li>– рекомендации о противопоказанных и доступных условиях и видах труда;</li> <li>– технические средства и услуги по реабилитации;</li> <li>– сведения о результатах осуществленных реабилитационных мероприятий</li> </ul>	И, С
2.42	Данные документа о беременности и родах и об отпусках по уходу за ребенком	<ul style="list-style-type: none"> <li>– Ф.И.О.;</li> <li>– данные документа, подтверждающего неполучения пособий супругом (вид, номер, дата выдачи);</li> <li>– срок постановки на учет по беременности<sup>4</sup>;</li> <li>– данные документа, подтверждающего постановку на учет по беременности в ранние сроки (вид, номер, дата выдачи)<sup>5</sup></li> </ul>	И
2.43	Данные документа, подтверждающего необходимость выплаты материальной помощи	<ul style="list-style-type: none"> <li>– Ф.И.О.;</li> <li>– данные документа, необходимого для подтверждения выплаты материальной помощи (вид, номер, дата выдачи)</li> </ul>	И
2.44	Сведения о наличии денежных обязательств	<ul style="list-style-type: none"> <li>– Ф.И.О.;</li> <li>– размер взыскиваемой суммы;</li> <li>– срок денежных обязательств;</li> <li>– данные документа, подтверждающего наличие обязательств (вид, номер, дата выдачи)</li> </ul>	И
<b>3</b>	<b>Персональные данные близких родственников кандидатов для трудоустройства на вакантную должность и (родственников) сотрудников</b>		
3.1	Сведения о годе рождения	<ul style="list-style-type: none"> <li>– Ф.И.О.;</li> <li>– год рождения</li> </ul>	И
3.2	Сведения о степени родства	<ul style="list-style-type: none"> <li>– Ф.И.О.;</li> <li>– степень родства</li> </ul>	И
3.3	Контактные данные	<ul style="list-style-type: none"> <li>– номер телефона</li> </ul>	И
<b>4</b>	<b>Персональные данные исполнителей, подрядчиков, агентов и иных лиц, являющихся стороной по договорам гражданско-правового характера (физических лиц, индивидуальных предпринимателей), за исключением заемщиков, поручителей и залогодателей</b>		
4.1	Паспортные данные или данные иного документа, удостоверяющего личность	<ul style="list-style-type: none"> <li>– Ф.И.О.;</li> <li>– наименование документа, удостоверяющего личность;</li> <li>– серия и номер документа;</li> <li>– дата выдачи документа;</li> <li>– наименование органа, выдавшего документ;</li> <li>– код подразделения</li> </ul>	И

<sup>4, 3</sup> Указанные сведения предоставляются матерью ребенка

№ п/п	Группа персональных данных	Содержание сведений	Категория ПДн <sup>3</sup>
4.2	Сведения о дате и месте рождения, пол	<ul style="list-style-type: none"> <li>- Ф.И.О.;</li> <li>- дата рождения;</li> <li>- место рождения;</li> <li>- пол</li> </ul>	И
4.3	Контактные данные	<ul style="list-style-type: none"> <li>- Ф.И.О.;</li> <li>- номер телефона (мобильный, домашний, рабочий);</li> <li>- e-mail</li> </ul>	И
4.4	Сведения о месте жительства	<ul style="list-style-type: none"> <li>- Ф.И.О.;</li> <li>- адрес регистрации по месту жительства, в том числе предыдущие адреса</li> </ul>	И
4.5	Данные свидетельства государственного пенсионного страхования	<ul style="list-style-type: none"> <li>- Ф.И.О.;</li> <li>- номер свидетельства ОПС (СНИЛС)</li> </ul>	И
4.6	Данные свидетельства о постановке на учет в налоговом органе	<ul style="list-style-type: none"> <li>- Ф.И.О.;</li> <li>- дата постановки на учет в налоговом органе;</li> <li>- ИНН;</li> <li>- наименование и код налогового органа</li> </ul>	И
4.7	Банковские реквизиты	<ul style="list-style-type: none"> <li>- Ф.И.О.;</li> <li>- реквизиты банка;</li> <li>- номер текущего, расчетного счета</li> </ul>	И
4.8	Сведения о договоре гражданско-правового характера	<ul style="list-style-type: none"> <li>- Ф.И.О.;</li> <li>- дата заключения договора;</li> <li>- номер договора;</li> <li>- срок действия договора</li> </ul>	И
4.9	Сведения о вознаграждении	<ul style="list-style-type: none"> <li>- Ф.И.О.;</li> <li>- размер вознаграждения</li> </ul>	И
4.10	Сведения об отчислениях в Фонд пенсионного и социального страхования Российской Федерации	<ul style="list-style-type: none"> <li>- Ф.И.О.;</li> <li>- страховой стаж;</li> <li>- размер страховых взносов</li> </ul>	И
4.11	Сведения об исчисленных, удержанных и перечисленных в бюджетную систему Российской Федерации налогах	<ul style="list-style-type: none"> <li>- Ф.И.О.;</li> <li>- размер налоговых перечислений</li> </ul>	И
4.12	Сведения о трудовой деятельности	<ul style="list-style-type: none"> <li>- Ф.И.О.;</li> <li>- наименование работодателя, адрес;</li> <li>- период работы;</li> <li>- должность;</li> <li>- причина увольнения</li> </ul>	И

### Общие и частные цели обработки персональных данных

Общие цели обработки персональных данных:

№ п/п	Категория субъектов персональных данных	Цели обработки персональных данных
1	Кандидаты для трудоустройства на вакантные должности	Рассмотрение резюме и подбор кандидатов для трудоустройства на вакантную должность в Банк
2	Сотрудники	Заключение, сопровождение, изменение, расторжение трудовых договоров, которые являются основанием для возникновения, изменения или прекращения трудовых отношений между сотрудниками и Банком
		Исполнение Банком обязательств, возникающих из трудовых договоров
		Исполнение Банком обязанностей, предусмотренных действующим законодательством Российской Федерации
3	Близкие родственники кандидатов для трудоустройства на вакантную должность / сотрудники	Получение дополнительной информации при рассмотрении резюме и подборе кандидатов для трудоустройства на вакантную должность в Банк
		Исполнение Банком обязанностей, предусмотренных действующим законодательством Российской Федерации
4	Исполнители, подрядчики, агенты и иные лица, являющиеся стороной по договорам гражданско-правового характера, (физические лица, индивидуальные предприниматели)	Заключение договора
		Исполнение Банком обязательств, предусмотренных по договору
		Исполнение Банком обязанностей, предусмотренных действующим законодательством Российской Федерации

Частные цели обработки персональных данных:

№ п/п	Категория субъектов персональных данных	Цели обработки персональных данных	Группы персональных данных <sup>6</sup>
1	Кандидаты для трудоустройства на вакантные должности	Осуществление связи с кандидатом для трудоустройства на вакантную должность в Банк	1.1
		Установление соответствия кандидата для трудоустройства на вакантную должность в Банк требованиям вакансии	1.7, 1.8, 1.9, 1.11, 1.12
		Оценка возможности и определение условий для заключения трудового договора с кандидатом для трудоустройства на вакантную должность в Банк	1.2, 1.3, 1.10, 1.11
		Проверка добросовестности кандидата для трудоустройства на вакантную должность до приема на работу в Банк	1.2, 1.4, 1.5, 1.6, 1.12
2	Сотрудники	Осуществление связи с сотрудником	2.4
		Проверка добросовестности сотрудника в	2.1, 2.2, 2.3, 2.8, 2.15, 2.38

<sup>6</sup> Для каждой цели обработки персональных данных указаны конкретные группы персональных данных в соответствии с Перечнем ПДн (приложение 1), обработка которых осуществляется в указанных целях.

№ п/п	Категория субъектов персональных данных	Цели обработки персональных данных	Группы персональных данных <sup>6</sup>
		период испытания при приеме на работу в Банк	
		Заключение, изменение, расторжение трудовых договоров, которые являются основанием для возникновения, изменения или прекращения трудовых отношений между сотрудниками и Банком	2.1, 2.2, 2.3, 2.5, 2.6, 2.7, 2.15, 2.16, 2.8, 2.10, 2.11, 2.12, 2.14, 2.18, 2.19, 2.20, 2.22, 2.27, 2.39
		Осуществление расчета и выплаты или удержания денежных средств (заработной платы, премий, надбавок, компенсаций, пособий)	2.17, 2.22, 2.23, 2.24, 2.26, 2.27, 2.28, 2.29, 2.30, 2.31, 2.32, 2.33, 2.34, 2.35, 2.40, 2.42, 2.44
		Ведение первичной учетной документации по учету труда и его оплаты	2.1, 2.2, 2.3, 2.4, 2.5, 2.6, 2.7, 2.9, 2.10, 2.16, 2.18, 2.19, 2.20, 2.22, 2.23, 2.24, 2.25, 2.27, 2.30, 2.31, 2.32, 2.33, 2.34, 2.35, 2.41, 2.43
		Ведение воинского учета сотрудников	2.10, 2.11
		Исчисление и уплата (перечисление) страховых взносов в Фонд пенсионного и социального страхования Российской Федерации	2.12, 2.36
		Исчисление, удержание, перечисление налогов в бюджетную систему Российской Федерации	2.13, 2.37
		Подготовка и подача сведений по обязательному квотированию рабочих мест	2.41
		Организация пропускного и внутриобъектового режима на территории зданий и отдельных помещений Банка	2.20, 2.21
		Исполнение Банком обязанностей, предусмотренных Федеральным законом от 25.12.2008 №273-ФЗ «О противодействии коррупции», в частности информирование нанимателя (работодателя) государственного или муниципального служащего по последнему месту его службы о заключении с ним трудового договора	2.2, 2.8, 2.18, 2.20
3	Близкие родственники кандидатов для трудоустройства на вакантную должность и сотрудников	Ведение первичной учетной документации по учету труда	3.1, 3.2
		Осуществление связи с родственниками для информирования о несчастном случае	3.3
4	Исполнители, подрядчики, агенты и иные лица, являющиеся стороной по договорам гражданско-правового характера, (физические лица, индивидуальные предприниматели) за исключением заемщиков, поручителей и залогодателей	Осуществление связи с лицом, являющимся стороной по договору гражданско-правового характера	4.3
		Заключение, изменение, расторжение договоров гражданско-правового характера, которые являются основанием для возникновения, изменения или прекращения отношений с Банком	4.1, 4.2, 4.4, 4.8
		Осуществление расчета и выплаты денежных средств	4.7, 4.8
		Исчисление и уплата (перечисление) страховых взносов в Фонд пенсионного и социального страхования Российской Федерации	4.5, 4.10

№ п/п	Категория субъектов персональных данных	Цели обработки персональных данных	Группы персональных данных <sup>6</sup>
		Исчисление, удержание, перечисление налогов в бюджетную систему Российской Федерации	4.6, 4.11
		Исполнение Банком обязанностей, предусмотренных Федеральным законом от 25.12.2008 №273-ФЗ «О противодействии коррупции», в частности информирование нанимателя (работодателя) государственного или муниципального служащего по последнему месту его службы о заключении с ним договора гражданско-правового характера	4.2, 4.8, 4.12

**Правовое основание получения персональных данных, обрабатываемых в Банке**

№ п/п	Категория субъектов персональных данных	Правовое основание обработки персональных данных
1	Кандидаты для трудоустройства на вакантные должности	<p>Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных» (пункт 5 части 1 статьи 6)</p> <p>Согласие субъекта персональных данных на обработку персональных данных</p>
2	Сотрудники	<p>Трудовой договор</p> <p>Трудовой кодекс Российской Федерации (статьи 57, 65, 86, 87, 88, 228)</p> <p>Постановление Правительства Российской Федерации от 27.11.2006 № 719 «Об утверждении Положения о воинском учете» (раздел 3)</p> <p>Федеральный закон от 15.12.2001 № 167-ФЗ «Об обязательном пенсионном страховании» (пункт 2 статьи 14)</p> <p>Налоговый кодекс Российской Федерации</p> <p>Федеральный закон от 25.12.2008 № 273-ФЗ «О противодействии коррупции»</p> <p>Федеральный закон от 24.11.1995 № 181-ФЗ «О социальной защите инвалидов в Российской Федерации»</p> <p>Постановление Государственного комитета Российской Федерации по статистике от 05.01.2004 № 1 «Об утверждении унифицированных форм первичной учетной документации по учету труда и его оплаты»</p> <p>Согласие субъекта персональных данных на обработку персональных данных</p>
3	Близкие родственники кандидатов для трудоустройства на вакантные должности и сотрудников	<p>Трудовой кодекс Российской Федерации (статья 228)</p> <p>Постановление Государственного комитета Российской Федерации по статистике от 05.01.2004 № 1 «Об утверждении унифицированных форм первичной учетной документации по учету труда и его оплаты»</p> <p>Согласие субъекта персональных данных на обработку персональных данных</p>
4	Исполнители, подрядчики, агенты и иные лица, являющиеся стороной договоров гражданско-правового характера, заключенных с Банком, (физические лица, индивидуальные предприниматели) за исключением заемщиков, поручителей и залогодателей	<p>Гражданско-правовой договор</p> <p>Гражданский кодекс Российской Федерации</p> <p>Налоговый кодекс Российской Федерации</p> <p>Федеральный закон от 25.12.2008 № 273-ФЗ «О противодействии коррупции»</p>

Текст  
**Согласия на обработку персональных данных**  
 (обязательная форма)

**Я свободно**, своей волей и в своем интересе даю ПАО БАНК «СИАБ», расположенному по адресу: 196084, г. Санкт-Петербург, ул. Черниговская, д. 8, лит. А, пом. 1-Н, (далее — «Банк») согласие (далее — «Согласие») на обработку следующих персональных данных (далее — «ПД»):

фамилия, имя, отчество, паспортные данные, номер телефона, адрес проживания, адрес электронной почты,

а также иных ПД, содержащихся в документах, предоставленных мною в рамках взаимодействия с Банком посредством использования мной мессенджеров, а также в заявке на банковский продукт, оформленной в сети Интернет, или в любых других документах, в том числе путем направления сообщений (озвучивания сведений) посредством каналов связи, либо ставших известными Банку от партнеров Банка или из сети Интернет или других источников в следующих целях:

— рассмотрение Банком возможности заключения со мной любых договоров о предоставлении банковских продуктов;

— проверка достоверности указанных мной сведений;

— хранение и перевозка документов, содержащих мои ПД и банковскую тайну, в соответствии с требованиями законодательства Российской Федерации;

— получение заключений и консультаций в любой форме, касающихся заключения, исполнения договоров о предоставлении банковских продуктов и реализации Банком своих прав и обязанностей по таким договорам;

— улучшение качества обслуживания, банковских продуктов, предлагаемых Банком на рынке финансовых услуг;

— улучшение привлекательности сайта Банка в сети Интернет;

— направление мне предложений о заключении договоров о предоставлении банковских продуктов и (или) информации о них;

— установление моих контактных данных для целей направления мне информационных сообщений;

Согласен(а) на направление рекламных сообщений по любым каналам связи, в том числе сетям электросвязи, и контактам, предоставленным мной Банку, в соответствии с ч. 1 ст. 18 закона от 13.03.2006 № 238-ФЗ «О рекламе»

Не согласен(а) на направление рекламных сообщений

— заключения мной и третьими лицами (партнерами Банка, оказывающими услуги его клиентам) договоров о получении продуктов и услуг партнера, получения консультаций третьих лиц об оказываемых ими услугах (предоставляемых ими сервисах);

— иные цели, которые будут указаны в заключенных между мною и Банком договорах о предоставлении банковских продуктов, иных документах.

○ **Я информирован(а)**, что обработка ПД может осуществляться Банком путем совершения с ними любого действия (операции) или совокупности действий (операций), осуществляемых на бумажных и (или) электронных носителях с использованием и (или) без использования средств автоматизации, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), в том числе при поручении обработки ПД третьим лицам, в том числе лицам, входящим в один банковский холдинг с Банком (аффилированным лицам Банка), обезличивание, блокирование, удаление, уничтожение ПД.

○ **Согласен(-на)** на передачу Банком ПД третьим лицам, в том числе: \_\_\_\_\_

\_\_\_\_\_, иным операторам связи, лицам, привлекаемым Банком для оказания услуг контакт-центра в целях проведения опроса для улучшения качества обслуживания, исследования удовлетворенности услугами Банка, информирования клиентов о предложениях Банка и привлечение потенциальных клиентов на обслуживание в Банк, а также лицам, входящим в один банковский холдинг с Банком (аффилированным лицам Банка) и лицам, входящим в один банковский холдинг с Банком (аффилированным лицам Банка), в целях, определенных Согласием. Я согласен(-на), что Банк вправе поручить обработку моих ПД другому лицу на основании заключаемого с этим лицом договора.

○ **Согласен(-на)** на использование любой предоставленной мною контактной информации Банком, третьими лицами по поручению Банка (включая лиц, привлекаемых Банком для оказания услуг контакт-центра и предоставляющих Банку права на использование программного обеспечения в целях привлечения потенциальных клиентов на обслуживание и аккумулирования информации о клиентах



с использованием такого программного обеспечения), либо без поручения при оказании мне услуг, для сообщения мне любой информации, касающейся заключения заключенных со мной или в моих интересах договоров.

○ Указывая в заявке на банковский продукт, оформленной в сети Интернет и (или) любых предоставляемых Банку документах сведения о третьих лицах (супруге, представителе, выгодоприобретателе и (или) иных лицах), **я поручаю** Банку осуществлять обработку предоставленных им ПД указанных лиц с целью принятия Банком решения о заключении со мной и (или) с третьими лицами договоров о предоставлении банковских продуктов, а также последующей реализации прав и обязанностей по таким договорам.

○ **Я подтверждаю**, что мной получено согласие таких лиц на обработку мною (включая передачу Банку) и Банком их ПД, предоставленных Банку, а также что до указанных лиц доведена информация в соответствии с требованиями Федерального закона «О персональных данных» (далее — «Закон»).

○ **Я ознакомлен(а)**, что обработка ПД осуществляется Банком в соответствии с особенностями и правилами, установленными Законом, постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», а также постановлением Правительства Российской Федерации от 1 ноября 2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных». Обработка ПД осуществляется Банком с соблюдением требований режима конфиденциальности и безопасности, требований к защите ПД в соответствии с Законом, также Банком выполняются требования, предусмотренные ч. 5 ст. 18, ст. 18.1, ч. 3.1 ст. 21 Закона и иные нормы законодательства о персональных данных.

Требования к защите обрабатываемых ПД, в том числе необходимые правовые, организационные и технические меры по защите ПД от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления и иных неправомерных действий в отношении ПД определяются Банком самостоятельно с учетом требований ст. 19 Закона.

○ **Я подтверждаю** свое ознакомление с правом в течение срока действия настоящего поручения, в том числе до начала обработки ПД, запросить документы и иную информацию, подтверждающие принятые меры и соблюдение в целях исполнения моего поручения требований, установленных в соответствии с Законом.

○ **Я согласен(-на)**, что обработка ПД в указанных выше целях может осуществляться Банком на бумажных и электронных носителях с использованием или без использования средств автоматизации, а также с тем, что решение о предоставлении мне банковского продукта может быть принято путем исключительно автоматизированной обработки моих ПД. Я подтверждаю, что мне известен порядок принятия решения на основании исключительно автоматизированной обработки моих ПД и возможные юридические последствия такого решения, а также порядок защиты мной своих прав и законных интересов и возможность заявить возражения против такого решения, представив в Банк соответствующее заявление.

○ **Я согласен(-на)** на предоставление Банку операторами связи, в т.ч. указанными выше, сведений обо мне, как абоненте и (или) пользователе услуг связи и оказываемых мне услугах связи (включая фамилию, имя, отчество, псевдоним, иное обозначение абонента (пользователя); адреса абонента (пользователя), установки (пользователя), местонахождения окончного оборудования; абонентские номера, иные данные, идентифицирующие абонента (пользователя), окончное оборудование; сведения систем расчета за услуги связи, в том числе о соединениях, трафике, платежах и другие данные, позволяющие идентифицировать абонента и (или) пользователя услуг связи или его абонентское устройство (за исключением сведений, составляющих тайну связи); результатов обработки имеющихся сведений в виде скоррингового балла.

○ **Я подтверждаю**, что мною получено письменное согласие субъекта персональных данных, чьи персональные данные содержатся в представленной в Банк информации, на обработку Банком этих персональных данных по поручению в указанных выше целях, а также гарантирую, что субъект персональных данных уведомлен об обработке его персональных данных Банком. Все подтверждающие документы будут представлены мною в Банк с согласия субъекта персональных данных, чьи персональные данные содержатся в таких документах. Также подтверждаю и согласен с тем, что я несу все неблагоприятные последствия, связанные с неполучением мною такого согласия от субъекта персональных данных.

Согласие дано сроком на 10 (десять) лет с даты его предоставления. По истечении указанного срока действие согласия считается продленным на каждые следующие 10 (десять) лет при условии отсутствия у Банка сведений о его отзыве. Согласие может быть отозвано путем предоставления в Банк письменного заявления клиента.

Настоящее Согласие может быть отозвано путем направления в Банк соответствующего заявления в письменной форме на адрес \_\_\_\_\_ (электронный адрес или принимаются исключительно в письменном виде на бумажном носителе?).

В случае отзыва мной Согласия Банк прекращает обработку ПД, а также обеспечивает прекращение такой обработки третьими лицами.

В случае отзыва мной настоящего Согласия Банк вправе продолжить обработку моих ПД без моего согласия в случаях, порядке и объеме, предусмотренных Законом.

*Подпись/расшифровка подписи/дата*

## **Формирование состава средств защиты персональных данных**

1. С целью установления методов и способов защиты, необходимых для обеспечения безопасности персональных данных, производится классификация информационных систем.

При проведении классификации учитываются следующие данные:

- категория (состав) обрабатываемых ПДн;
- объем (количество субъектов) обрабатываемых ПДн;
- наличие подключений к сетям общего пользования;
- режим обработки ПДн;
- местонахождение технических средств информационной системы, в которой производится обработка ПДн.

2. По результатам анализа, для каждой информационной системы, в которой производится обработка ПДн, присваивается класс, согласно рекомендациям нормативных документов регулирующих и контролирующих органов. Результат классификации оформляется актом и хранится в ДКИ.

3. Состав рекомендуемых средств защиты информации, в зависимости от класса информационной системы и типовых моделей угроз, определен нормативными документами регулирующих органов и уточняется на основе анализа уязвимостей и возможных угроз с оценкой ущерба от реализации угроз. Состав актуальных угроз оформляется актом и хранится в ДКИ.

4. Сформированный состав средств защиты ПДн, обеспечивающий нейтрализацию предполагаемых актуальных угроз, проходит проверку готовности, установку и ввод в эксплуатацию с обязательным оформлением необходимой документации и обучением лиц, использующих средства защиты информации.

5. Средства защиты информации и лица, допущенные к работе с ПДн, подлежат обязательному учету.

6. Контроль за соблюдением условий использования средств защиты информации и заключения по фактам нарушения конфиденциальности ПДн обеспечивают поддержание защищенности ПДн на необходимом уровне. Все контрольные мероприятия оформляются актами, содержащими анализ выявленных несоответствий или нарушений, рекомендации по их устранению и ответственных за их выполнение.

7. Результатом процесса формирования, внедрения, эксплуатации средств защиты информации является декларирование соответствия или сертификация (аттестация) по требованиям безопасности информации.

8. В случае изменения в функционировании информационных систем или изменениях в частной модели угроз производится повторный процесс формирования состава средств защиты информации и оценка соответствия требованиям по безопасности информации.

**Нормативные правовые акты, определяющие сроки архивного хранения документов, содержащих персональные данные, в Банке**

№ п/п	Категория субъектов персональных данных	Нормативные правовые акты и сроки хранения
1	Кандидаты для трудоустройства на вакантные должности	<p>Федеральный закон от 22.10.2004 № 125-ФЗ «Об архивном деле в Российской Федерации» (пункт 1 статьи 17);            Приказ Росархива от 20.12.2019 N 236 «Об утверждении Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков их хранения»</p> <p>Срок хранения документов (анкет, автобиографий, листов по учету кадров, заявлений, рекомендательных писем) лиц, не принятых на работу – 5 лет</p> <p>Согласие на обработку персональных данных – 3 года после истечения срока его действия или отзыва</p>
2	Сотрудники	<p>Федеральный закон от 22.10.2004 № 125-ФЗ «Об архивном деле в Российской Федерации» (пункт 1 статьи 17);            Положение Росархива № 1, Банка России от 12.07.2022 № 801-П «Об утверждении Перечня документов, образующихся в процессе деятельности кредитных организаций, с указанием сроков их хранения»</p> <p>Сроки хранения:</p> <ul style="list-style-type: none"> <li>• личных дел (заявлений, копий приказов и выписок из них, копий личных документов, листов по учету кадров, анкет, аттестационных листов и другого) сотрудников – 75 лет;</li> <li>• трудовых договоров – 75 лет;</li> <li>• личных карточек сотрудников, в том числе временных сотрудников – 75 лет;</li> <li>• характеристик, резюме сотрудников, не вошедшие в состав личных дел – 5 лет;</li> <li>• не востребовавшихся подлинных личных документов (трудовых книжек, дипломов, аттестатов, удостоверений, свидетельств) – 75 лет;</li> <li>• документов (справок, докладных, служебных записок, копий приказов, выписок из приказов, заявлений и другого), не вошедших в состав личных дел – 5 лет;</li> <li>• командировочных удостоверений – 5 лет после возвращения из командировки (для сотрудников, направленных в командировки в районы Крайнего Севера и приравненные к ним местности, – 75 лет);</li> <li>• документов (служебных заданий, отчетов, переписки) о командировании сотрудников – 5 лет (для долгосрочных зарубежных командировок – 10 лет);</li> <li>• договоров о повышении квалификации сотрудников - 5 лет после истечения срока действия договора;</li> <li>• документов (сводных расчетных (расчетно-платежных) ведомостей и документов к ним), расчетных листов на выдачу заработной платы, пособий, гонораров, материальной помощи и других выплат - 5 лет (при отсутствии лицевых счетов – 75 лет);</li> <li>• лицевых карточек, счетов сотрудников – 75 лет;</li> <li>• отчетов по перечислению денежных сумм по государственному и негосударственному страхованию – постоянно;</li> <li>• реестров сведений о доходах физических лиц – 75 лет;</li> <li>• документов (постановлений, определений, актов, решений, протоколов, заключений, запросов, заявлений, переписки) о соблюдении норм законодательства, конфликтах, спорах, иных вопросах правового характера – 5 лет;</li> <li>• копий документов (исковых заявлений, доверенностей, актов, справок, докладных записок, ходатайств, протоколов, определений, постановлений, характеристик), представляемых в</li> </ul>

№ п/п	Категория субъектов персональных данных	Нормативные правовые акты и сроки хранения
		<p>правоохранительные, судебные органы, третейские суды – 5 лет после вынесения решения;</p> <ul style="list-style-type: none"> <li>• переписки по вопросам правоохранительного характера – 5 лет;</li> </ul> <p>согласие на обработку персональных данных – 3 года после истечения срока его действия или отзыва</p>
3	Близкие родственники кандидатов для трудоустройства на вакантные должности и сотрудников	<p>Федеральный закон от 22.10.2004 №125-ФЗ «Об архивном деле в Российской Федерации» (пункт 1 статьи 17);          Приказ Росархива от 20.12.2019 N 236 «Об утверждении Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков их хранения»</p> <p>Срок хранения:          анкет сотрудников (в составе личных дел) – 75 лет;          личных карточек сотрудников, в том числе временных сотрудников – 75 лет</p>
4	Исполнители, подрядчики, агенты и иные лица, являющиеся стороной договоров гражданско-правового характера, заключенных с Банком, (физические лица, индивидуальные предприниматели) за исключением заемщиков, поручителей и залогодателей	<p>Федеральный закон от 22.10.2004 №125-ФЗ «Об архивном деле в Российской Федерации» (пункт 1 статьи 17);          Приказ Росархива от 20.12.2019 N 236 «Об утверждении Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков их хранения»</p> <p>Срок хранения:          договоров, соглашений, не указанных в отдельных статьях Перечня – 5 лет после истечения срока действия договора, соглашения;          документов (расчетов, заключений, справок, переписки) к договорам, соглашениям – 5 лет после истечения срока действия договора, соглашения;          отчетов по перечислению денежных сумм по государственному и негосударственному страхованию – постоянно;          реестров сведений о доходах физических лиц – 75 лет;          документов (постановлений, определений, актов, решений, протоколов, заключений, запросов, заявлений, переписки) о соблюдении норм законодательства, конфликтах, спорах, иных вопросах правового характера – 5 лет;          копий документов (исковых заявлений, доверенностей, актов, справок, докладных записок, ходатайств, протоколов, определений, постановлений, характеристик), представляемых в правоохранительные, судебные органы, третейские суды – 5 лет после вынесения решения;          переписки по вопросам правоохранительного характера – 5 лет.</p>

**Порядок  
обеспечения непрерывности и реагирования на инцидент при эксплуатации  
технических средств и программного обеспечения, баз данных и средств защиты  
информации ИСПДн**

**1. Порядок реагирования на инцидент**

1.1. Под инцидентом понимается событие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн, а также потерей защищаемой информации.

Происшествие, вызывающее инцидент, может произойти в результате:

- непреднамеренных действий пользователей;
- преднамеренных действий пользователей и третьих лиц;
- нарушения правил эксплуатации технических средств ИСПДн;
- возникновения внештатных ситуаций и обстоятельств непреодолимой силы.

Все действия в процессе реагирования на инцидент должны документироваться ответственным за реагирование сотрудником в Системе JIRA.

1.2. Порядок действий сотрудников указан в Приложении 6 к настоящему Положению.

В кратчайшие сроки, не превышающие одного рабочего дня, ответственные за реагирование сотрудники предпринимают меры по восстановлению работоспособности.

Предпринимаемые меры должны быть согласованы с Заместителем Президента-Председателя Правления Банка по информационной безопасности. При необходимости, иерархия может быть нарушена с целью получения квалифицированной консультации в кратчайшие сроки.

**2. Меры обеспечения непрерывности работы и восстановления ресурсов при возникновении инцидентов****2.1. Технические меры.**

К техническим мерам обеспечения непрерывной работы и восстановления относятся:

- программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения инцидентов, такие как системы жизнеобеспечения;
- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных; системы контроля физического доступа.

**2.1.1. Системы жизнеобеспечения ИСПДн включают:**

- пожарные сигнализации и системы пожаротушения;
- системы вентиляции и кондиционирования;
- системы резервного питания.

Все критичные помещения Банка (помещения, в которых размещаются элементы ИСПДн и средства защиты) должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

2.1.2. Для выполнения требований по эксплуатации (температура, относительная влажность воздуха) программно-аппаратных средств ИСПДн в помещениях, где они установлены, должны применяться системы вентиляции и кондиционирования воздуха.

2.1.3. Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы ИСПДн, сетевое и коммуникационное оборудование, а также наиболее критичные рабочие станции должны подключаться к сети электропитания через источники бесперебойного питания (или встроенные аккумуляторы). В зависимости от необходимого времени работы ресурсов после потери питания могут применяться следующие методы резервного электропитания:

- локальные источники бесперебойного электропитания с различным временем питания для защиты отдельных компьютеров;
- источники бесперебойного питания с дополнительной функцией защиты от скачков напряжения;
- дублированные системы электропитания в устройствах (серверы, концентраторы, мосты и т. д.);
- резервные линии электропитания в пределах комплекса зданий;
- аварийные электрогенераторы.

Также могут применяться системы обеспечения отказоустойчивости:

- кластеризация;
- технология RAID.

2.1.4. Для обеспечения отказоустойчивости критичных компонентов ИСПДн при сбое в работе оборудования и их автоматической замены без простоев могут использоваться методы кластеризации, в частном случае территориально удаленные системы кластеров. Для защиты от

отказов отдельных дисков серверов, осуществляющих обработку и хранение защищаемой информации, должны использоваться технологии RAID, которые (кроме RAID-0) применяют дублирование данных, хранимых на дисках.

2.1.5. Система резервного копирования и хранения данных, должна обеспечивать хранение защищаемой информации на съемном машинном носителе информации (магнитной ленте, жестком диске и т.п.).

## **2.2. Организационные меры**

2.2.1. Резервное копирование и хранение данных должно осуществляться на периодической основе - для обрабатываемых персональных данных - не реже раза в неделю; для технологической информации - не реже раза в месяц; эталонные копии программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программные средства защиты), с которых осуществляется их установка на элементы ИСПДн - не реже раза в месяц, и каждый раз при внесении изменений в эталонные копии (выход новых версий).

2.2.2. Данные о проведении процедуры резервного копирования, должны отражаться в электронном журнале.

2.2.3. Носители, на которые произведено резервное копирование, должны быть пронумерованы и учтены: номером носителя, датой проведения резервного копирования.

2.2.4. Носители должны храниться в негорючем шкафу или помещении оборудованном системой пожаротушения.

2.2.5. Носители должны храниться не менее года, для возможности восстановления данных.

## **Инструкция по обработке персональных данных без использования средств автоматизации**

### **1. Порядок обработки ПДн**

1.1. Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных данных (далее - бумажные носители), в специальных разделах или на полях форм (анкет, бланков, т.п.).

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

1.3. При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению отдельной обработки персональных данных.

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

1.5. Уточнение персональных данных 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 персональными данными.

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

1.7. Необходимо обеспечивать отдельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

1.8. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются Приказом.

1.9. Для обеспечения физической сохранности бумажных носителей персональных данных (далее - документов), предотвращения их хищения, а также для недопущения разглашения содержащихся в них сведений, документы должны храниться в сейфах, шкафах или тумбах, запираемых на ключ.

1.10. Хранение открытых документов вместе с конфиденциальными документами разрешено только в случаях, когда они являются приложениями к конфиденциальным документам.

1.11. Рабочее место сотрудников, обрабатывающих ПДн, должно быть организовано таким способом, чтобы исключить просмотр документов с ПДн, лицами, которые не допущены к обработке ПДн.

1.12. Не разрешается хранение документов с ПДн в местах, не запираемых на ключ.

1.13. На столе сотрудников, обрабатывающих ПДн, должны быть только те документы, с которыми ведется непосредственно работа, все остальные должны быть убраны в сейф или шкафы.

1.14. Все документы, содержащие ПДн, после окончания рабочего дня, должны убираться в запираемые сейфы и шкафы.

1.15. Документы передаются на архивное хранение по достижении целей обработки.

### **2. Порядок уничтожения бумажных носителей ПДн**

2.1. Основанием для уничтожения бумажных носителей является:

- достижение целей обработки;
- отзыв согласия субъекта на обработку его ПДн;
- получение соответствующего запроса от субъекта ПДн;
- получение соответствующего указания от уполномоченного органа по защите прав

субъектов.

2.2. Экспертиза документов и массивов документов проводится раз в год путем изучения содержания документов. Цель проведения экспертизы – определить возможность уничтожения документов либо дальнейшие сроки их хранения.

2.3. Массивы документов (архивы, библиотеки и т.п.) уничтожаются под контролем комиссии по выполнению требований Федерального закона от 27 июля 2006 года №152-ФЗ «О персональных данных» (далее – Комиссия) после проведения экспертизы документов.

Комиссия назначается Приказом по Банку и является постоянно действующей. В Состав комиссии в обязательном порядке включается сотрудник ДКИ.

2.4. Уничтожение бумажных носителей ПДн производится с помощью шредера, сжигания документов или ручным способом, путем разрыва документа на малые части или иными методами, избранными Банком.

2.5. После уничтожения документов или массива документов членами Комиссии подписывается акт об уничтожении бумажных носителей ПДн, по форме определяемой Комиссией.

**3. Ответственность за соблюдение норм**, описанных в данном Приложении, возлагается на всех сотрудников, обрабатывающих ПДн, а периодический контроль за выполнением правил хранения - на их непосредственных руководителей.



## **Инструкция пользователя информационной системы персональных данных (ИСПДн)**

**1.** Пользователем информационной системы персональных данных Банка (далее – Пользователь) является сотрудник Банка, осуществляющий обработку персональных данных в ИСПДн.

**2.** Пользователь в своей работе руководствуется настоящей Инструкцией, внутренними нормативными и распорядительными документами Банка, с которыми он был ознакомлен при прохождении первичного инструктажа.

**3.** Пользователь несет персональную ответственность за свои действия.

**4.** Пользователь обязан:

– знать и выполнять требования «Положения о защите персональных данных», «Политики в отношении обработки персональных данных в ПАО БАНК «СИАБ»;

– знать и выполнять установленные требования по режиму обработки ПДн, учету, хранению и использованию носителей ПДн, обеспечению безопасности ПДн;

– соблюдать требования «Политики информационной безопасности» в отношении использования паролей;

– обеспечивать защиту персональных данных от несанкционированного доступа;

– блокировать АРМ в случае отсутствия на рабочем месте;

– информировать сотрудников ДКИ обо всех случаях (подозрениях) нарушения или несоблюдения требований по защите персональных данных или возникновения нестандартных ситуаций;

– оказывать необходимое содействие (в т. ч. давать устные и письменные объяснения) при проведении контрольных мероприятий.

**5.** Пользователю запрещается:

– разглашать обрабатываемые ПДн;

– разглашать информации об используемых средствах защиты персональных данных;

– допускать к обработке персональных данных сотрудников, не имеющих допуска;

– производить копирование ПДн на неучтенные носители;

– производить несанкционированное копирование ПДн на учтенные носители;

– оставлять рабочее место с активным приложением, в котором производится обработка персональных данных, без личного контроля;

– оставлять без личного контроля носители информации, содержащие персональные данные;

– сообщать и передавать третьим лицам личные пароли и атрибуты доступа к ресурсам ИСПДн.

**6.** За нарушение информационной безопасности по защите ПДн Пользователь несет ответственность согласно действующему законодательству РФ.

**Действия**  
**Пользователя информационной системы персональных данных (ИСПДн)**  
**и Ответственного за организацию обработки персональных данных**  
**при возникновении нештатных ситуаций**

1. Под нештатной ситуацией понимается событие, связанное со сбоем в функционировании элементов ИСПДн.

2. При реагировании на инцидент Пользователь должен правильно классифицировать критичность инцидента.

3. Критичность оценивается на основе следующей классификации:

— Уровень 1. Незначительный инцидент – локальное событие с ограниченным разрушением, которое не влияет на общую доступность элементов ИСПДн и средств защиты;

— Уровень 2. Авария – любой инцидент, который приводит или может привести к прерыванию работоспособности отдельных элементов ИСПДн и средств защиты;

— Уровень 3. Катастрофа – любой инцидент, приводящий к полному прерыванию работоспособности всех элементов ИСПДн и средств защиты, к уничтожению, блокированию, неправомерной модификации или компрометации защищаемых персональных данных, а также к угрозе жизни пользователей ИСПДн.

4. При возникновении нештатной ситуации любого уровня Пользователь обязан оповестить Ответственного за организацию обработки персональных данных, сообщив характер аварийной ситуации, масштаб ситуации по предварительной субъективной оценке.

5. Ответственный за организацию обработки персональных данных обеспечивает:

— ознакомление сотрудника с данным приложением к «Положению о защите персональных данных» в срок, не превышающий 3-х рабочих дней с момента выхода нового сотрудника на работу;

— обучение пользователей, имеющих доступ к ресурсам ИСПДн, порядку действий при возникновении аварийных ситуаций.

6. Пользователи ИСПДн должны получить базовые знания в следующих областях:

— пожаротушение;

— эвакуация людей;

— защита материальных и информационных ресурсов;

— методы оперативной связи со службами спасения и руководителями структурных подразделений;

— выключение оборудования, электричества.

**Порядок  
проведения инструктажа лиц, допущенных к работе  
с информационной системой персональных данных (ИСПДн)**

Сотрудник, которому для выполнения своих трудовых обязанностей предоставляется доступ к ИСПДн, должен быть ознакомлен:

1. С законодательством РФ о персональных данных:
  - Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;
  - Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
  - Постановлением Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» (для сотрудников, обрабатывающих персональные данные, в том числе без использования средств автоматизации).
  
2. С внутренними нормативными документами Банка в отношении обработки персональных данных:
  - «Политикой в отношении обработки персональных данных в ПАО БАНК «СИАБ»;
  - «Положением о защите персональных данных»;
  - «Инструкцией по обеспечению сохранности информации ограниченного доступа»;
  - «Инструкцией по учету и хранению съемных носителей персональных данных»;
  - «Порядком контроля доступа в помещения Банка»;
  - «Положением об организации видеонаблюдения в Банке»;
  - «Инструкцией по рассмотрению обращений субъектов персональных данных и их законных представителей»;
  - «Регламентом по работе с обращениями, поступающими в адрес Банка»;
  - «Порядком ведения электронного кадрового документооборота».
  
3. С ответственностью за неисполнение требований законодательства РФ о персональных данных

Сотрудник, которому для выполнения своих трудовых обязанностей предоставляется доступ к ИСПДн, должен подписать обязательство о неразглашении персональных данных.