УТВЕРЖДАЮ

Временно исполняющая полномочия
и обязанности Председателя Правления
ООО «Эйч-эс-би-си Банк (РР)»
Е.В. Рогова

«15 » сентября 2021 г.

Политика ООО «Эйч-эс-би-си Банк (РР)» в отношении обработки персональных данных и сведения о реализуемых требованиях к защите персональных данных

Москва
2021

1 Общие положения

1.1. «Политика ООО «Эйч-эс-би-си Банк (РР)» в отношении обработки персональных данных и сведения о реализуемых требованиях к защите персональных данных» (далее – Политика) определяет общие принципы и порядок обработки персональных данных и меры по обеспечению их безопасности в ООО «Эйч-эс-би-си Банк (РР)» (далее – Банк).

Целью Политики является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну, четкое и неукоснительное соблюдение требований законодательства Российской Федерации в области персональных данных.

1.2. Политика разработана в соответствии с положениями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», другими законодательными и нормативными правовыми актами, определяющими порядок работы с персональными данными и требования к обеспечению их безопасности.

1.3. В Политике используются следующие термины и определения:

Автоматизированная обработка персональных данных	Обработка персональных данных с помощью средств вычислительной техники
База персональных данных	Упорядоченный массив персональных данных, независимый от вида материального носителя информации и используемых средств его обработки (архивы, картотеки, электронные базы данных)
Банк	ООО «Эйч-эс-би-си Банк (РР)»
Биометрические персональные данные	Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность, и которые используются оператором для установления личности субъекта персональных данных
Блокирование персональных данных	Временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных)
Группа HSBC	Эйч-эс-би-си Холдингс плс, компания, созданная и действующая в соответствии с законодательством Англии и Уэльса, и/или Эйч-эс-би-си Банк плс, банк, созданный и действующий в соответствии с законодательством Англии и Уэльса, и каждая из компаний, входящих в группу, контролируемую этим банком.
Дата-центр	Специализированная организация, предоставляющая услуги по размещению серверного и сетевого оборудования, сдаче серверов (в том числе виртуальных) в аренду, а также по подключению к сети Интернет.
Доступ к персональным данным	Ознакомление определенных лиц (в том числе работников) с персональными данными субъектов, обрабатываемыми Банком, при условии сохранения конфиденциальности этих сведений
Законодательство	Законодательство Российской Федерации

Информационная безопасность	Состояние защищенности информации, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность при ее обработке в информационных системах
Информационная система персональных данных	Совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств
Контрагент	Сторона договора с Банком, не являющаяся работником Банка
Конфиденциальность персональных данных	Обязательное для соблюдения Банком или иным получившим доступ к персональным данным лицом требование не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено законодательством Российской Федерации
Лицо, ответственное за обеспечение безопасности персональных данных в информационных системах персональных данных	Работник Банка, в обязанности которого входит организация процессов обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных Банка
Лицо, ответственное за организацию обработки персональных данных	Работник Банка, в обязанности которого входит организация процессов обработки персональных данных в Банке
Материальные носители	Материальный объект, используемый для закрепления и хранения на нем информации, содержащей персональные данные, в том числе в преобразованном виде
Обезличивание персональных данных	Действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных
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
Общедоступные персональные данные	Персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе или с его согласия, а также персональные данные, которые подлежат обязательному опубликованию или раскрытию в соответствии с законодательством Российской Федерации

Оператор	Государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующее и (или) осуществляющее обработку персональных данных, а также определяющее цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными; в Положении под оператором понимается Банк, если иное не указано специально
Персональные данные	Любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)
Предоставление персональных данных	Действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц
Распространение персональных данных	Действия, направленные на раскрытие персональных данных неопределенному кругу лиц
Специальные категории персональных данных	Сведения, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья
Субъект персональных данных	Физическое лицо, к которому относятся персональные данные
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

1.4. В Политике используются следующие сокращения:

ПДн	Персональные данные
ИСПДн	Информационная система персональных данных

2. Статус Банка и категории субъектов, чьи персональные данные обрабатываются Банком

1.1 Субъекты персональных данных

2.1.1. Банк является оператором в отношении ПДн следующих физических лиц:

- работников Банка, с которыми заключены или были заключены трудовые договоры, в том числе те, с которыми трудовые и гражданско-правовые договоры уже расторгнуты (далее – **Работники**);

- близких родственников, супругов работников Банка, в том числе бывших супругов, которым выплачиваются алименты, и лиц, находящихся на иждивении работников (далее – **Члены семей работников**);
- соискателей вакантных должностей Банка (кандидатов для приема на работу Банком), представивших лично или через специализированные организации по подбору персонала (кадровые агентства), в том числе через специализированные сайты в сети интернет, свои резюме или анкеты (далее – **Соискатели**);
- бывших клиентов-физических лиц, включая владельцев банковских счетов, вкладчиков, заемщиков, клиентов по торговым операциям на рынке ценных бумаг, залогодателей и поручителей по кредитам, клиентов разовых услуг (потребителей услуг Банка, не требующих открытия счета: обмен валют, денежные переводы, платежи), плательщиков и получателей по счетам (далее – **Бывшие клиенты**);
- бенефициарных владельцев, представителей, работников, собственников, акционеров клиентов Банка-юридических лиц (далее – **Связанные лица**);
- конрагентов–физических лиц и представителей контрагентов Банка, являющихся юридическими лицами и индивидуальными пердпринимателями, с которыми у Банка существуют договорные отношения, с которыми Банк намерен вступить в договорные отношения или которые намерены вступить в договорные отношения с Банком, а также иных лиц (работников, участников (акционеров), учредителей, бенефициаров, выгодоприобретателей, контрагентов, членов руководящих органов, не являющихся работниками, лиц, действующих в интересах контрагента на основании доверенностей и т.д.), персональные данные которых могут передаваться Банку в целях заключения и исполнения договоров с контрагентами, а также в целях проверки Банком контрагентов в качестве благонадежных для заключения с ними договоров и совершения иных сделок и в рамках противодействия легализации (отмыванию) доходов полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового уничтожения (далее – **Представители контрагентов**);
- Посетителей сайта hsbc.ru, не зарегистрировавшихся и не прошедших авторизацию (далее – **Посетители сайта**);
- представителей всех вышеперечисленных физических лиц, обращающихся в Банк по поручению и от имени субъектов ПДн (далее – **Представители субъектов**);
- посетителей охраняемых помещений Банка, не имеющих права постоянного входа в эти помещения (далее – **Посетители**).

2.1.2. Банк является лицом, осуществляющим передачу на регулярной основе персональных данных субъектов другим операторам, к которым относятся (не исчерпывая):

- органы власти и местного самоуправления, государственные внебюджетные фонды, в которые перечисляются средства Работников или средства для зачисления на счет Работников (инспекции Федеральной налоговой службы, территориальные отделения Пенсионного фонда Российской Федерации, Федерального фонда обязательного медицинского страхования, Фонда социального страхования Российской Федерации др.);
- Банк России, Государственная корпорация «Агентство страхования вкладов», Росфинмониторинг и иные органы, которым Банком предоставляется информация, в том числе относящаяся к ПДн и составляющая банковскую тайну, в случаях, предусмотренных статьей 26 Федерального закона от 02.12.1990 № 395-1 «О банках и банковской деятельности»;
- органы статистики, военные комиссариаты, операторы сввязи, которым ПДн предоставляются (передаются) в случаях, предусмотренных законодательством.

Указанным выше операторам ПДн предоставляются (передаются) в объеме, определенном законодательством, соответствующими органами власти и государственными внебюджетными фондами в пределах их полномочий. Специального согласия субъектов на такую передачу этих ПДн не требуется.

2.1.3. Банк не является оператором в отношении ПДн, которые его раотники, клиенты и поставщики, а также их представители самостоятельно и по собственной инициативе вносят в информационные системы других банков (компаний) группы HSBC, включая информационные системы материнского банка HSBC.

2.1.4. Банк не несет ответственности за достоверность ПДн, включенных в свои базы данных его контрагентами, в том числе – другими банками (компаниями) группы HSBC, а также компаниями, которые оказывают Банку информационные услуги, за правомерность включение таких ПДн в базы данных и предоставление их контрагентами Банку на основании договора или в соответствии с корпоративными правилами группы HSBC.

1.2 Принципы и цели обработки персональных данных

Обработка ПДн Банком осуществляется в соответствии со следующими принципами:

2.2.1. Законная и справедливая основа обработки ПДн. Банк принимает все необходимые меры по выполнению требований законодательства, не обрабатывает ПДн в случаях, когда это не допускается законодательством и не требуется для достижения определенных Банком целей, не использует ПДн во вред субъектам.

2.2.2. Ограничение обработки ПДн достижением конкретных, заранее определённых и законных целей. Целями обработки ПДн Банком являются:

- в отношении Работников – исполнение заключенных трудовых договоров, в том содействие в трудоустройстве и продвижении по службе, обеспечение личной безопасности работников, контроль количества и качества выполняемой работы и обеспечение сохранности имущества, расчет и выплата заработной платы, иных вознаграждений, расчет и перечисление налогов и страховых взносов; выполнение требований корпоративной политики по учёту персонала банков группы HSBC за рубежом, профессиональном обучении, позволяющем соблюдать международные стандарты и требования группы HSBC, а также иностранных регуляторов при командировках и работе в других юрисдикциях; предоставление работникам дополнительных услуг за счет работодателя (перечисление доходов на банковские карты работников, страхование, обеспечение командировок, предоставление парковочного места и пр.), контроль за аффилированностью в случаях, установленных Банком России, размещение сведений о Работниках и их фотографических изображений в маркетинговых материалах, выполнение требований нормативных правовых актов органов государственного статистического учета;
- в отношении Членов семей работников – предоставление работникам льгот и гарантий, предусмотренных законодательством для лиц, имеющих (усыновивших) детей, лиц с семейными обязанностями; выполнение требований трудового законодательства об информировании родственников о несчастных случаях; добровольное медицинское страхование за счет работодателя; страхование жизни и страхование от несчастных случаев, негосударственное пенсионное обеспечение, предоставляемые работникам в рамках внутренних компенсационных политик Банка, выполнение требований нормативных правовых актов органов государственного статистического учета;
- в отношении Соискателей – принятие решения о возможности замещения вакантных должностей кандидатами, наиболее полно соответствующими требованиям Банка; соблюдение требований применимого законодательства, в том числе и при

трансграничной передаче данных (в случае, если такая передача предусмотрена корпоративными правилами группы HSBC);

- в отношении Бывших клиентов – выполнение законодательства о противодействии легализации (отмыванию) доходов, полученных преступным путем и финансированию терроризма, соблюдение требований законодательства, в том числе и при трансграничной передаче данных, а также обеспечение защиты прав и интересов клиентов;
- в отношении Представителей контрагентов – заключение и исполнение договоров с контрагентами, проверка Банком контрагентов в качестве благонадежных для заключения с ними договоров и совершения иных сделок и в рамках противодействия легализации (отмыванию) доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового уничтожения;, соблюдение требований применимого законодательства, в том числе при трансграничной передаче данных (в случае, если такая передача предусмотрена корпоративными правилами группы HSBC);
- в отношении Посетителей сайта – предоставление возможности использовать сайт, просматривать его страницы; получение статистических данных о посещении сайта;
- в отношении Представителей субъектов – выполнение Банком действий по поручению Представителей субъектов ПДн, соблюдение требований законодательства, в том числе и при трансграничной передаче данных (в случае, если такая передача предусмотрена корпоративными правилами группы HSBC);
- в отношении Посетителей – обеспечение возможности прохода в офисы Банка и его обособленных структурных подразделений лиц, не имеющих постоянных пропусков, соблюдение требований законодательства, в том числе и при трансграничной передаче данных (в случае, если такая передача предусмотрена корпоративными правилами группы HSBC).

2.2.3. Обработка только тех ПДн, которые отвечают заранее объявленным целям их обработки. Соответствие содержания и объёма обрабатываемых ПДн заявленным целям обработки. Недопущение обработки ПДн, не совместимой с целями сбора ПДн, а также избыточных по отношению к заявленным целям их обработки ПДн. Банк не собирает и не обрабатывает ПДн, не требующиеся для достижения целей, указанных в п.2.2.2 Политики, не использует ПДн субъектов в каких-либо целях, отличных от указанных выше.

2.2.4. Недопущение объединения баз данных, содержащих ПДн, обработка которых осуществляется в целях, не совместимых между собой.

2.2.5. Обеспечение точности, достаточности и актуальности ПДн по отношению к целям обработки ПДн. Банк принимает все разумные меры по поддержке актуальности обрабатываемых ПДн, включая, но не ограничиваясь, реализацией права каждого субъекта получать для ознакомления свои ПДн и требовать от Банка их уточнения, блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленных выше целей обработки.

2.2.6. Хранение ПДн в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен законодательством или договором, стороной которого является субъект ПДн, а также согласием субъекта персональных данных на обработку данных.

2.2.7. Уничтожение ПДн по достижении заявленных целей их обработки или в случае утраты необходимости в достижении этих целей, при невозможности устранения Банком допущенных нарушений установленного законодательством порядка обработки ПДн, отзыве согласия на обработку субъектом ПДн, истечении срока обработки ПДн, установленных

локальными актами Банка, согласием на обработку ПДн, если иное не предусмотрено законодательством или договорами с субъектами.

2.2.8. ПДн, обрабатываемые Банком, могут являться банковской или иной охраняемой законодательством тайной. В этом случае на эти данные распространяются требования и ограничения, установленные соответствующим применимым законодательством.

1.3 Условия обработки персональных данных

2.3.1. Обработка ПДн Банком допускается в следующих случаях:

2.3.1.1. При наличии согласия субъекта ПДн на обработку его ПДн. Порядок получения Банком согласия субъекта ПДн определен в разделе 3.2 Политики.

2.3.1.2. Обработка ПДн необходима для достижения целей, предусмотренных законом, а также для осуществления и выполнения возложенных законодательством на Банк функций, полномочий и обязанностей. К таким случаям в том числе, относится, не исчерпывая их, обработка специальных категорий ПДн Работников для достижения целей, предусмотренных трудовым и пенсионным законодательством, обработка ПДн Бывших клиентов, идентификация Представителей контрагентов в соответствии с Федеральным законом от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».

2.3.1.3. Для исполнения договора, стороной которого является субъект ПДн, для заключения договора по инициативе субъекта ПДн. Такими договорами, не исчерпывая, являются, трудовые договоры с Работниками Банка и гражданско-правовые договоры с контрагентами-физическими лицами.

Преддоговорной работой является работа по подбору персонала, в которой согласие субъекта на обработку ПДн подтверждается собственноручно заполненной анкетой Соискателя или анкетой (резюме), переданной им Банку, в специализированную организацию по подбору персонала, размещенной Соискателем на специализированных сайтах в сети интернет или присланной Соискателем в Банк по электронной почте.

2.3.1.4. Обработка ПДн необходима для осуществления прав и законных интересов Банка или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъектов ПДн.

2.3.1.5. Обработка ПДн осуществляется в статистических или иных исследовательских целях при условии обязательного обезличивания ПДн.

2.3.1.6. Обработка ПДн, разрешенных субъектом персональных данных для распространения с условием соблюдения установленных субъектом ограничений и запретов.

2.3.1.7. ПДн подлежат опубликованию или обязательному раскрытию в соответствии с законодательством.

2.3.2. Банк не раскрывает третьим лицам и не распространяет ПДн без согласия субъекта ПДн, если иное не предусмотрено законодательством, договором с субъектом ПДн, не указано в полученном от него согласии на обработку ПДн.

2.3.3. Банк не обрабатывает ПДн, относящиеся к специальным категориям и касающиеся расовой и национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья (за исключением сведений, относящихся к вопросу о возможности выполнения Работником трудовой функции и необходимых для целей, определенных законодательством о государственной социальной помощи, законодательством об обязательных видах страхования, трудовым, пенсионным и страховым законодательством), интимной жизни, о членстве Работников в общественных объединениях или их профсоюзной деятельности, за исключением случаев, прямо предусмотренных законодательством.

2.3.4. Обработка ПДн о судимости может осуществляться Банком исключительно в случаях и в порядке, установленных применимым законодательством.

2.3.5. Банк не обрабатывает биометрические ПДн.

2.3.6. Банк не принимает решения, порождающие юридические последствия в отношении субъекта ПДн или иным образом затрагивающие права и законные интересы субъекта, на основании исключительно автоматизированной обработки Банк. Данные, имеющие юридические последствия или затрагивающие права и законные интересы субъекта, такие, как размер начисленных доходов, налогов и иных отчислений и другие, подлежат перед их использованием проверке со стороны уполномоченных работников Банка.

2.3.7. Банк осуществляет трансграничную передачу ПДн Работников в рамках информационного обмена с банками (компаниями) группы HSBC на территорию Великобритании, являющейся стороной «Конвенции о защите частных лиц в отношении автоматизированной обработки данных личного характера» № ETS-108 в целях выполнения требований корпоративной политики по учёту персонала банков группы HSBC за рубежом, о профессиональном обучении.

2.3.8. Банк осуществляет трансграничную передачу ПДн на территорию стран, определяемых клиентами Банка при выполнении поручений клиентов, в том числе на территорию стран, не обеспечивающих адекватную защиту прав субъектов ПДн, в частности, при выполнении операций, исполнении сделок и поручений клиентов, осуществлении платежей и переводе денежных средств за рубеж, в необходимом для исполнения такого поручения объеме и составе.

2.3.9. Все ПДн, в отношении которых осуществляется трансграничная передача, при их сборе записываются (фиксируются, приобщаются) в базы данных, находящиеся в офисах Банка на территории Российской Федерации, в которых происходит, при необходимости, также их уточнение, изменение или обновление перед трансграничной передачей изменившихся ПДн.

3. Обработка персональных данных

Обработка ПДн Банком осуществляется смешанным способом – как без использования средств автоматизации с фиксацией ПДн на отдельных материальных носителях ПДн, в специальных разделах или на полях форм (бланков), так и с использованием средств автоматизации.

3.1. Конфиденциальность персональных данных

3.1.1. Работниками Банка, получившими доступ к ПДн, должна быть обеспечена конфиденциальность таких данных.

Обеспечение конфиденциальности не требуется в отношении:

- ПДн после их обезличивания;
- общедоступных ПДн.

3.1.2. Банк вправе с согласия субъекта поручить обработку ПДн другому лицу, если иное не предусмотрено законодательством, на основании заключаемого с этим лицом договора, предусматривающего в качестве существенного условия обязанность лица, осуществляющего обработку ПДн по поручению Банка, соблюдать принципы и правила обработки ПДн, предусмотренные законодательством. Объем передаваемых ПДн другому лицу для обработки и используемые этим лицом способы обработки должны быть минимально необходимыми для выполнения им своих обязанностей перед Банком.

В поручении Банка должны быть определены перечень действий (операций) с ПДн, которые будут совершаться лицом, осуществляющим обработку ПДн, и цели обработки, должна

быть установлена обязанность такого лица соблюдать конфиденциальность ПДн и обеспечивать безопасность ПДн при их обработке, а также должны быть указаны требования к защите обрабатываемых ПДн в соответствии со статьей 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

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

3.1.4. Банк вправе разместить свои информационные системы персональных данных в дата-центре (облачной вычислительной инфраструктуре), у другого оператора, а также передать материальные носители персональных данных (документы, содержащие персональные данные) на хранение другому оператору. В этом случае в договор с дата-центром (провайдером облачных услуг, другим оператором) в качестве существенного условия может включаться требование о запрете доступа персонала дата-центра (провайдера облачных услуг, другого оператора) к ИСПДн и материальным носителям (документам) Банка, размещаемых в дата-центре (облачной инфраструктуре, у другого оператора), и тогда такое размещение (хранение) не рассматривается Банком как поручение обработки ПДн дата-центру (провайдеру облачных услуг, другому оператору) и не требует согласия субъектов ПДн. При передаче материальных носителей (документов, содержащих персональные данные) другому оператору Банк принимает меры по обеспечению возможности контроля за несанкционированным доступом к передаваемым на хранение документам.

3.2. Согласие субъекта персональных данных на обработку своих персональных данных

3.2.1. Субъект ПДн принимает решение о предоставлении его ПДн Банку и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку ПДн должно быть конкретным, информированным и сознательным и может предоставляться субъектом в любой позволяющей подтвердить факт его получения форме, если иное не установлено законодательством.

3.2.2. В случае получения согласия на обработку ПДн от Представителя субъекта ПДн полномочия данного представителя на дачу согласия от имени субъекта ПДн проверяются Банком.

3.2.3. В случае получения Банком ПДн от контрагента на основании и в целях заключения и/или исполнения заключенного между ними договора ответственность за правомерность и достоверность ПДн, а также за получение согласия Представителей контрагента на передачу их ПДн Банку несет контрагент, передающий ПДн, что закрепляется в договоре Банка с контрагентом.

3.2.4. Банк, получивший ПДн от контрагента, не принимает на себя обязательства по информированию субъектов (их представителей), ПДн которых ему переданы, о начале обработки ПДн, поскольку обязанность осуществить соответствующее информирование субъекта при заключении договора и/или при получении согласия на такую передачу несет передавший ПДн контрагент. Данная обязанность контрагента включается в договор, заключаемый с ним Банком.

3.2.5. Специально выраженного согласия Работника на обработку его ПДн не требуется, так как обработка необходима для исполнения договора, стороной которого является Работник-субъект ПДн, за исключением случаев, когда необходимо получение согласия Работника в письменной форме для конкретных случаев обработки ПДн. К случаям, требующим согласия Работника в письменной форме, относятся (не исчерпывая):

- включение ПДн Работника в общедоступные источники ПДн, в том числе – размещение их на официальном сайте Банка в сети Интернет, за исключением случаев, когда опубликование и обязательное раскрытие ПДн установлено законодательством;
- обработка специальных категорий ПДн, в том числе обработка сведений о состоянии здоровья Работника, не связанных с возможностью выполнения Работником трудовой функции и не являющихся необходимыми для достижения целей, предусмотренных пенсионным законодательством;
- трансграничная передача ПДн в страны, не обеспечивающие адекватной защиты прав субъектов ПДн, в том числе – банкам (компаниям) группы HSBC;
- получение ПДн Работников у третьих лиц, в том числе – с целью их проверки, а также в случаях, когда данные нельзя получить у самого Работника;
- передача ПДн Работника какой-либо третьей стороне, в том числе – передача его ПДн при направлении в служебные командировки, на обучение и повышение квалификации, для оформления виз, бронирования перевозок и размещения в гостиницах, предоставление ПДн другим банкам (компаниям) группы HSBC и т.п.;
- сообщение ПДн Работника третьим лицам в коммерческих целях, в том числе – компании, осуществляющей кадровый и воинский учет Работников, расчет начисляемой им заработной платы и иных доходов Работников, банкам, открывающим и обслуживающим платежные карты для начисления заработной платы и иных доходов Работника, страховым компаниям, осуществляющим добровольное страхование Работников за счет Банка как работодателя и т.п.;
- передача ПДн арендодателю и (или) частной охранной организации с целью обеспечения внутриобъектового режима.

3.2.6. Не требуется согласия Работников, в отношении которых Банком должен проводиться контроль за их аффилированностью в соответствии с требованиями Банка России, на получение от иных лиц сведений, необходимых для проведения контроля за аффилированностью.

3.2.7. ».

3.2.8. Специально выраженного согласия Членов семей работников на обработку их ПДн не требуется, если такая обработка осуществляется на основании законодательства (для получения алиментов, оформления социальных выплат, предоставления льгот и гарантий и пр.), а также выполняется Банком как работодателем в соответствии с требованиями Трудового кодекса РФ и органов государственного статистического учета, а также в случаях, когда Члены семей работников являются выгодоприобретателями, в том числе – застрахованными лицами по договорам, заключенным Банком как страховщиком в пользу Членов семей работников. Во всех остальных случаях необходимо получение доказываемого (подтверждаемого) согласия Членов семей работников на обработку их ПДн Банком.

3.2.9. Специально выраженного согласия Соискателей на обработку их ПДн не требуется, так как обработка необходима в целях заключения трудового договора по инициативе Соискателя как субъекта ПДн, за исключением случаев, когда необходимо получение согласия Соискателя в письменной форме для конкретных случаев обработки ПДн. В случае принятия решения о приеме Соискателя на работу или об отказе Соискателю в приеме на работу его ПДн уничтожаются в течение 30 дней с даты принятия такого решения.

3.2.10. Специально выраженного согласия Бывших клиентов на обработку их ПДн не требуется, т.к. такая обработка ведется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем и финансированию терроризма.

3.2.11. ПДн Представителей конрагентов, содержащиеся в единых государственных реестрах юридических лиц и индивидуальных предпринимателей, являются открытыми и общедоступными, за исключением сведений о номере, дате выдачи и органе, выдавшем документ, удостоверяющий личность физического лица. Обеспечения их конфиденциальности и согласия субъектов на обработку таких данных не требуется.

Во всех остальных случаях необходимо получение согласия субъектов ПДн, являющихся Представителями контрагентов, за исключением лиц, подписавших договоры с Банком, предоставивших доверенности на право действовать от имени и по поручению контрагентов Банка и тем самым совершивших конклюдентные действия, подтверждающие их согласие с обработкой ПДн, указанных в тексте договора, доверенности. Согласие у своего представителя на передачу его ПДн Банку и обработку им этих ПДн может получить контрагент в порядке, описанным в п.3.2.3 Политики. В этом случае получение Банком согласия субъекта на обработку его ПДн не требуется.

3.2.12. Согласие Посетителей сайта дается путем простановки соответствующей отметки во всплывающем окне (чек-боксе) на сайте hsbc.ru или путем закрытия баннера, уведомляющего о использовании фалов cookie.

3.2.13. Согласие Представителя субъекта на обработку его ПДн дается в форме конклюдентных действий, выразившихся в предоставлении доверенности на право действовать от имени и по поручению субъектов ПДн и документа, удостоверяющего его личность.

3.2.14. Согласие Посетителя на обработку его ПДн дается в форме конклюдентных действий, выразившихся в предоставлении документа, удостоверяющего личность, и сообщении сведений, запрашиваемых у него при посещении офисов Банка.

3.2.15. В случае необходимости получения согласия субъекта на обработку ПДн в письменной форме такое согласие может быть получено в форме электронного документа, подписанного электронной подписью в соответствии с требованиями, установленными законодательством.

3.2.16. Согласие субъектов на предоставление их ПДн не требуется при получении Банком в рамках установленных полномочий мотивированных запросов судов, Банка России, налоговых органов, органов прокуратуры, правоохранительных органов, органов следствия и дознания, органов безопасности, от государственных инспекторов труда при осуществлении ими государственного надзора и контроля за соблюдением трудового законодательства, и иных органов, уполномоченных запрашивать информацию в соответствии с компетенцией, предусмотренной законодательством.

Мотивированный запрос должен включать в себя указание цели запроса, ссылку на правовые основания запроса, в том числе подтверждающие полномочия органа, направившего запрос, а также перечень запрашиваемой информации.

3.2.17. В случае поступления запросов из организаций, не обладающих соответствующими полномочиями, Банк обязан получить доказываемое согласие от субъекта, не являющегося Работником Банка, на предоставление его ПДн, и предупредить лиц, получающих ПДн, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, а также требовать от этих лиц подтверждения того, что это правило будет (было) соблюдено. Порядок получения согласия работников Банка на передачу их ПДн иным лицам описан в пункте 3.2.5 Политики.

3.2.18. Согласие на обработку ПДн, обработка которых не установлена требованиями законодательства или не требуется для исполнения договора с Банком, стороной которого является субъект ПДн, может быть отозвано субъектом ПДн. Банк вправе продолжить обработку ПДн после отзыва субъектом согласия на обработку при наличии оснований, предусмотренных

п.п.2-11 ч.1 ст.6, ч.2 ст.10 и ч.2 ст.11 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

3.2.19. Во всех случаях обязанность предоставить доказательство получения согласия субъекта ПДн на обработку его ПДн или доказательство наличия оснований, указанных в Федеральном законе от 27.07.2006 № 152-ФЗ «О персональных данных», возлагается на Банк.

4. Права субъектов персональных данных

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

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

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

5. Сведения о реализуемых требованиях к защите персональных данных

5.1. Безопасность ПДн, обрабатываемых Банком, обеспечивается реализацией правовых, организационных и технических мер, необходимых и достаточных для обеспечения требований законодательства в области защиты ПДн.

5.2. Правовые меры включают:

- разработку локальных актов Банка, реализующих требования законодательства, в том числе – Политики Банка в отношении обработки ПДн;
- отказ от любых способов обработки ПДн, не соответствующих определенным в Политике целям и требованиям законодательства.

5.3. Организационные меры включают:

- назначение лица, ответственного за организацию обработки ПДн;
- назначение лица, ответственного за обеспечение безопасности ПДн в ИСПДн;
- ограничение состава работников Банка, имеющих доступ к ПДн, и организацию разрешительной системы доступа к ним;
- ознакомление работников Банка, непосредственно осуществляющих обработку ПДн, с положениями законодательства о ПДн, в том числе с требованиями к защите ПДн, с Политикой, другими локальными актами Банка по вопросам обработки ПДн;
- обучение всех категорий работников, непосредственно осуществляющих обработку ПДн, правилам работы с ними и обеспечения безопасности обрабатываемых данных;
- определение в должностных инструкциях работников Банка обязанностей по обеспечению безопасности обработки ПДн и ответственности за нарушение установленного порядка;
- регламентацию процессов обработки ПДн;
- организацию учёта материальных носителей ПДн и их хранения, обеспечивающих предотвращение хищения, подмены, несанкционированного копирования и уничтожения;

- определение типа угроз безопасности ПДн, актуальных для ИСПДн с учетом оценки возможного вреда субъектам ПДн, который может быть причинен в случае нарушения требований безопасности, определение уровня защищенности ПДн, требований к защите ПДн при их обработке в ИСПДн, исполнение которых обеспечивает установленные уровни защищенности ПДн;
- определение угроз безопасности ПДн при их обработке в ИСПДн, формирование на их основе частной модели (моделей) актуальных угроз;
- размещение технических средств обработки ПДн в пределах охраняемой территории;
- ограничение допуска посторонних лиц в помещения Банка, недопущение их нахождения в помещениях, где ведется работа с ПДн и размещаются технические средства их обработки, без контроля со стороны работников Банка.

5.4. Технические меры включают:

- реализацию требований к защите ПДн при их обработке в ИСПДн, исполнение которых обеспечивает установленные уровни защищенности ПДн, разработку на основе частной модели актуальных угроз и введение в эксплуатацию системы защиты ПДн для установленных Правительством Российской Федерации уровней защищенности ПДн при их обработке в информационных системах;
- использование для нейтрализации актуальных угроз средств защиты информации, прошедших процедуру оценки соответствия;
- оценку эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию ИСПДн;
- реализацию разрешительной системы доступа работников к ПДн, обрабатываемым в информационных системах, программно-аппаратным и программным средствам защиты информации;
- регистрацию и учёт действий с ПДн пользователей информационных систем, где обрабатываются ПДн;
- выявление вредоносного программного обеспечения (применение антивирусных программ) на всех узлах информационной сети Банка, обеспечивающих соответствующую техническую возможность;
- безопасное межсетевое взаимодействие (применение межсетевого экранирования);
- обнаружение фактов несанкционированного доступа к ПДн и принятием мер, в том числе мер по обнаружению, предупреждению и ликвидации последствий компьютерных атак на ИСПДн и по реагированию на компьютерные инциденты в них;
- шифрование передаваемых по незащищенным каналам связи, в том числе через сеть интернет, ПДн как при получении их от клиентов и поставщиков с целью исполнения договора с ними, так и при их отправке клиентам и поставщикам;
- восстановление ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним (систему резервного копирования и восстановления ПДн);
- периодическое проведение мониторинга действий пользователей, разбирательств по фактам нарушения требований безопасности ПДн;
- контроль за выполнением настоящих требований (самостоятельно или с привлечением на договорной основе организаций, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации) не реже 1 раза в 3 года.

6. Заключительные положения

6.1. Иные обязанности и права Банка как оператора персональных данных и лица, организующего их обработку по поручению других операторов, определяются законодательством Российской Федерации в области персональных данных.

6.2. Работники Банка, виновные в нарушении требований законодательства в области ПДн и Политики, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством ответственность.

6.3. Юридические лица, нарушившие договорные обязательства по обеспечению конфиденциальности ПДн, несут гражданско-правовую ответственность в соответствии с законодательством Российской Федерации.

6.4. Актуализация[1] Политики проводится в следующих случаях:

- при изменении законодательства в области обработки и защиты ПДн;
- в случаях получения предписаний на устранение несоответствий, затрагивающих область действия Политики;
- по решению руководства Банка;
- при изменении организационной структуры Банка, касающейся подразделений, задействованных в реализации Политики;
- при изменении структуры информационных и/или телекоммуникационных систем (или введении новых), применении новых технологий обработки ПДн;
- при появлении необходимости в изменении процесса обработки ПДн, связанной с бизнес-деятельностью Банка;
- по фактам возникновения инцидентов, уязвимостей, иных значимых событий ИБ, по решению руководства Банка.

Все изменения в настоящий документ вносятся и утверждаются в установленном в Банке порядке.

[1] Под актуализацией понимается проверка Политики на соответствие требованиям законодательства Российской Федерации, отраслевых стандартов, нормативных документов Банка, требованиям бизнес-деятельности и т.п. По результатам актуализации в текст Политики могут быть внесены изменения.