АКЦИОНЕРНОЕ ОБЩЕСТВО
СБЕРБАНК - ТЕХНОЛОГИИ

УТВЕРЖДЕНА
Приказом АО «СберТех»
от 08.11.2021 № 204

«08» ноября 2021г. ПТ СБТ 09-015 2.01

ПОЛИТИКА

ОБРАБОТКА И ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

Москва, 2021

ОГЛАВЛЕНИЕ

1. ЦЕЛЬ РАЗРАБОТКИ

Настоящая Политика разработана с целью реализации требований законодательства РФ в области обработки и обеспечения безопасности ПДн, обеспечения защиты прав и свобод человека и гражданина при обработке его ПДн в Компании.

2. ОБЩИЕ ПОЛОЖЕНИЯ

3.1. Настоящая Политика разработана в соответствии с Конституцией РФ, Федеральным законом от 19.12.2005 № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных», Трудовым кодексом РФ от 30.12.2001 № 197-ФЗ, Федеральным законом №152-ФЗ от 27.07.2006 «О персональных данных», Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Постановлением Правительства РФ № 687 от 15.09. 2008 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», иными федеральными законами и подзаконными актами РФ, определяющими случаи и особенности обработки персональных данных и обеспечения безопасности и конфиденциальности такой информации, а также в соответствии с Регламентом № 2016/679 Европейского парламента и Совета Европейского Союза «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС (Общий Регламент о защите персональных данных)».

3.2. Положения настоящей Политики являются обязательными для исполнения всеми работниками Компании, осуществляющими обработку и (или) защиту ПДн.

3.3. Положения настоящей Политики являются основой для организации работы по обработке и защите ПДн в Компании, в том числе, для разработки ВНД, регламентирующих обработку и защиту ПДн в Компании.

3.4. В случае если отдельные положения настоящей Политики войдут в противоречие с действующим законодательством о ПДн, применяются положения действующего законодательства.

3.5. Запросы Субъектов ПДн в отношении обработки их ПДн Компанией принимаются:

- по адресу Компании: 117105, РФ, Москва, Новоданиловская набережная, д. 10;
- по адресу e-mail: sbt-privacy@sberbank.ru.

3.6. Настоящая Политика является документом, к которому обеспечивается неограниченный доступ. Для обеспечения неограниченного доступа Политика, в частности, опубликована на официальном сайте Компании в сети Интернет по адресу: http://sber-tech.com.

3. СПИСОК РОЛЕЙ

Ответственный за организацию обработки ПДн: должностное лицо, назначенное РД Компании ответственным за организацию процесса обработки ПДн, а также за организационно-правовую защиту ПДн в Компании в соответствии с требованиями законодательства о ПДн.

Ответственный за обеспечение безопасности ПДн: должностное лицо, назначенное РД Компании ответственным за техническую, а также организационно-техническую защиту ПДн.

4. ЦЕЛЬ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Компания осуществляет обработку ПДн в следующих целях:

- подбор персонала, содействие в трудоустройстве;
- ведение кадровой работы и организация учета работников;
- регулирование трудовых и иных, связанных с ними отношений;
- организация командировок работников;
- проведение корпоративных мероприятий;
- прикрепление к зарплатному проекту Компании;
- прикрепление к программам страхования Компании;
- прикрепление к негосударственной пенсионной программе Компании;
- организация обучения;
- проведение выходных интервью;
- проведение всесторонних проверок процессов, при реализации которых обрабатываются/могут обрабатываться ПДн;
- организация предоставления траспортных услуг работникам Компании в рамках производственной необходимости;
- предоставления парковочных мест для отдельных категорий работников Компании;
- организация отправки грузов и корреспонденции;
- предоставление корпоративной мобильной связи для отдельных категорий работников;
- осуществление административно- хозяйственной деятельности;
- обеспечение безопасности и сохранности имущества;
- работа с обращениями Субъектов ПДн;
- управление рисками в деятельности Компании;
- исполнение требований Федеральных законов и подзаконных актов РФ;
- иные законные цели.

4.2. Содержание и объем обрабатываемых ПДн соответствуют заявленной цели их обработки. Компанией осуществляются необходимые мероприятия по недопущению обработки ПДн, избыточных по отношению к заявленной цели их обработки.

5. ОСНОВНЫЕ ПРИНЦИПЫ ОБРАБОТКИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. Компания осуществляет обработку ПДн на основе принципов:

- законности и справедливости обработки ПДн;
- законности заранее определенных конкретных целей и способов обработки ПДн;
- соответствия целей обработки ПДн целям, заранее определенным и заявленным при сборе ПДн;
- соответствия содержания и объема обрабатываемых ПДн целям обработки ПДн;
- точности и достаточности ПДн, а в необходимых случаях и актуальности по отношению к целям обработки;
- недопустимости обработки ПДн, избыточных по отношению к целям, заявленным при сборе ПДн;
- недопустимости объединения баз данных, содержащих ПДн, обработка которых осуществляется в целях, несовместимых между собой;
- хранения ПДн в форме, позволяющей определить Субъекта ПДн, не дольше, чем этого требуют цели их обработки, если срок хранения ПДн не установлен федеральным законом, договором, стороной которого, либо выгодоприобретателем по которому является Субъект ПДн;

- уничтожения или обезличивания ПДн по достижении целей их обработки, или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

5.2. В рамках обработки ПДн для Компании и Субъектов ПДн определены следующие права:

5.2.1. Субъект ПДн имеет право:

- получать информацию, касающуюся обработки его ПДн, в порядке, форме и сроки, установленные законодательством о ПДн;
- требовать уточнения своих ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, недостоверными, незаконно полученными, не являются необходимыми для заявленной цели обработки или используются в целях, не заявленных ранее при предоставлении Субъектом ПДн согласия на обработку ПДн;
- принимать предусмотренные законом меры по защите своих прав;
- отозвать свое согласие на обработку ПДн,

а также иные права, предусмотренные законодательством о ПДн.

5.2.2. Компания имеет право:

- обрабатывать ПДн Субъекта ПДн в соответствии с заявленной целью;
- требовать от Субъекта ПДн предоставления достоверных ПДн, необходимых для исполнения договора, идентификации Субъекта ПДн, а также в иных случаях, предусмотренных законодательством о ПДн;
- ограничить доступ Субъекта ПДн к его ПДн в случае, если доступ Субъекта ПДн к его ПДн нарушает права и законные интересы третьих лиц, а также в иных случаях, предусмотренных законодательством РФ;
- ПДн из общедоступных источников;
- обрабатывать ПДн, разрешенные субъектом ПДн для распространения (с учетом установленных Субъектом ПДн запретов и условий обработки);
- осуществлять обработку ПДн, подлежащих опубликованию или обязательному раскрытию в соответствии с законодательством РФ;
- поручить обработку ПДн другому лицу с согласия Субъекта ПДн,

а также иные права, предусмотренные законодательством о ПДн.

5.3. Компания обеспечивает защиту ПДн на основе следующих принципов:

- недопущения неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении ПДн;
- соблюдения конфиденциальности ПДн (за исключением случаев, когда ПДн разрешены для распространения Субъектом ПДн, либо распространяются на основании закона);
- реализация права на доступ к ПДн.

6. ОСОБЕННОСТИ И УСЛОВИЯ ОБРАБОТКИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. Для достижения целей обработки ПДн Компания осуществляет следующие операции с ПДн: сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (предоставление, доступ, распространение), обезличивание, блокирование, удаление, уничтожение.

6.2. Компания осуществляет смешанную обработку ПДн.

6.3. Доступ к обрабатываемым ПДн предоставляется только тем работникам Компании,

которым он необходим для исполнения ими своих должностных обязанностей. Перечень таких работников определяется соответствующим РД Компании. Содержание и уровень персональной ответственности определен нижестоящим ВНД Компании в области обработки ПДн.

6.4. Компания осуществляет необходимые мероприятия для поддержания точности, достаточности, а в необходимых случаях актуальности ПДн по отношению к целям их обработки.

6.5. Компания осуществляет обработку ПДн с согласия Субъекта ПДн на обработку его ПДн. Исключение составляют случаи, когда Компания имеет право осуществлять обработку ПДн без согласия Субъекта ПДн на обработку его ПДн а именно:

- для достижения целей, предусмотренных законодательством РФ, для осуществления и выполнения возложенных законодательством РФ на Компанию, как Оператора ПДн, обязанностей;
- для исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством РФ;
- для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является Субъект ПДн, а также для заключения договора по инициативе Субъекта ПДн или договора, по которому Субъект ПДн будет являться выгодоприобретателем или поручителем;
- для осуществления прав и законных интересов Компании или третьих лиц с соблюдением условий, при которых не нарушаются права и свободы Субъекта ПДн;
- в случае если обработка ПДн необходима для защиты жизни, здоровья или иных жизненно важных интересов Субъекта ПДн, если получение согласия субъекта ПДн невозможно;
- в случае если обработка ПДн необходима для научной, творческой деятельности при условии, что при этом не нарушаются права и законные интересы Субъекта ПДн;
- в случае если обработка ПДн осуществляется в статистических или иных исследовательских целях, при условии обязательного обезличивания ПДн;
- обрабатываемые ПДн подлежат опубликованию или обязательному раскрытию в соответствии с федеральным законом.

6.6. Компания не обрабатывает специальные категории ПДн, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни, медицинской информации, отражающей состояние здоровья Субъекта ПДн, за исключением случаев, определенных законодательством РФ. Компания не осуществляет обработку биометрических ПДн.

6.7. Компания не обрабатывает данные о членстве Субъекта ПДн в общественных объединениях, религиозных организациях и его профсоюзной деятельности.

6.8. Компания вправе поручить обработку ПДн другому (третьему) лицу с согласия Субъекта ПДн, если иное не предусмотрено законодательством РФ. Такая обработка ПДн осуществляется третьим лицом на основании заключенного между Компанией и ним договора (поручения оператора), в котором должны быть определены:

- цели обработки ПДн;
- перечень действий (операций) с ПДн, которые будут совершаться третьим лицом, осуществляющим обработку ПДн;
- обязанности третьего лица соблюдать конфиденциальность ПДн и обеспечивать их безопасность при обработке, а также требования к защите обрабатываемых ПДн.

Компания несет ответственность перед Субъектом ПДн за действия лиц, которым она поручает обработку этих ПДн.

6.9. Компания может обрабатывать ПДн Субъекта ПДн по поручению другого оператора на

основании заключаемого с ним договора (поручение оператора).

6.10. Компания не раскрывает третьим лицам и не предоставляет им ПДн без согласия Субъекта ПДн, за исключением случаев, установленных законодательством РФ.

6.11. Компания может осуществлять трансграничную передачу ПДн Субъектов ПДн.

6.12. Компания не принимает решений, порождающих юридические последствия в отношении Субъекта ПДн или иным образом затрагивающих его права и законные интересы, на основании исключительно автоматизированной обработки ПДн.

6.13. Компания не обрабатывает ПДн в целях политической агитации.

6.14. Компания обрабатывает ПДн не дольше, чем этого требуют цели обработки ПДн.

6.15. В Компании соответствующим РД Компании назначаются Ответственный за организацию обработки ПДн, а также Ответственный за обеспечение безопасности ПДн.

6.16. В Компании разрабатываются и актуализируются ВНД, РД по вопросам обработки и защиты ПДн.

6.17. В Компании регулярно проводится получение объективного перечня условий и факторов, создающих угрозы безопасности ПДн при их обработке в ИСПДн.

6.18. Обеспечение безопасности обрабатываемых ПДн осуществляется Компанией путем реализации технических, организационно-технических и организационно-правовых мероприятий по защите персональных данных в соответствии с требованиями законодательства о ПДн. Система информационной безопасности Компании непрерывно развивается и совершенствуется.

6.19. Ввод в эксплуатацию новых ИСПДн производится только после выполнения процедур оценки эффективности принимаемых мер по обеспечению безопасности обрабатываемых в них ПДн.

6.20. В Компании принимаются необходимые технические, организационно-технические, а также организационно-правовые меры защиты ПДн, обеспечивающие:

- предотвращение несанкционированного доступа к ПДн и (или) передачи их лицам, не имеющим права на доступ к ПДн;
- своевременное обнаружение фактов несанкционированного доступа к ПДн;
- предупреждение возможности неблагоприятных последствий нарушения порядка доступа к ПДн;
- недопущение воздействия на технические средства обработки ПДн, в результате которого нарушается их функционирование;
- возможность незамедлительного восстановления ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- постоянный контроль за обеспечением уровня защищенности ПДн;
- нахождение на территории РФ баз данных, содержащих ПДн, с использованием которых осуществляются сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение ПДн граждан РФ.

6.21. В Компании реализуются меры по организации обработки и обеспечению безопасности ПДн, обрабатываемых без средств автоматизации.

6.22. Обработка ПДн прекращается при достижении целей такой обработки, если иное не предусмотрено законодательством РФ, договором, стороной которого, выгодоприобретателем или поручителем по которому является Субъект ПДн, или иным соглашением между Компанией и Субъектом ПДн. При отзыве Субъектом ПДн согласия на обработку его ПДн, Компания вправе продолжить обработку ПДн без согласия Субъекта ПДн, если такая обработка предусмотрена договором, стороной которого, выгодоприобретателем или поручителем по которому является Субъект ПДн, иным соглашением между Компанией и Субъектом ПДн, либо если Компания вправе

осуществлять обработку ПДн без согласия Субъекта ПДн на основаниях, предусмотренных законодательством о ПДн.

7. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

7.1. Компания несет ответственность за соответствие обработки и защиты ПДн требованиям законодательства о ПДн.

7.2. Работники Компании несут гражданско-правовую, административную и иную ответственность за несоблюдение принципов и условий обработки ПДн, а также за разглашение или незаконное использование ПДн в соответствии с законодательством о ПДн, а также ВНД/РД Компании.

ПРИЛОЖЕНИЕ 1. СПИСОК ТЕРМИНОВ И ОПРЕДЕЛЕНИЙ

Компания: Акционерное общество «Сбербанк – Технологии», АО «СберТех».

Автоматизированная обработка ПДн: обработка ПДн с помощью средств автоматизации (в т.ч. средств вычислительной техники).

Административно-хозяйственная деятельность: процессы, направленные на текущее обеспечение деятельности Компании товарно-материальными ценностями (осуществление закупок канцтоваров, офисного оборудования, расходных материалов, хозяйственных товаров, услуг связи и т.п.); на организацию документооборота (ведение архива, библиотек, баз данных); на организацию эксплуатации зданий, помещений, территорий (содержание, уборка, оформление и ремонт помещений); на организацию рабочего процесса.

Законодательство о ПДн: совокупность нормативно-правовых актов, указанных в Приложении 3, а также иные действующие федеральные законы и подзаконные акты РФ, регулирующие отношения в сфере обработки и защиты ПДн.

Защита ПДн: комплекс мероприятий технического, организационно-технического и организационного-правового характера, направленных на обеспечение безопасности ПДн.

Информационная система ПДн: совокупность содержащихся в базах данных ПДн и обеспечивающих их обработку информационных технологий и технических средств.

Конфиденциальность ПДн: обязательное для соблюдения оператором или иным получившим доступ к ПДн лицом требование не допускать их распространение без согласия субъекта ПДн или наличия иного законного основания.

Неавтоматизированная обработка ПДн: обработка ПДн, осуществляемая при непосредственном участии человека без использования средств автоматизации (в т.ч. средств вычислительной техники).

Обработка ПДн: любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с ПДн, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн.

Оператор ПДн (оператор): государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку ПДн, а также определяющие цели обработки ПДн, состав ПДн, подлежащих обработке, действия (операции), совершаемые с ПДн.

Персональные данные: любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту ПДн).

Персональные данные, разрешенные Субъектом ПДн для распространения: ПДн, доступ неограниченного круга лиц к которым предоставлен Субъектом ПДн путем дачи согласия на обработку ПДн, разрешенных Субъектом ПДн для распространения в порядке, предусмотренном Законодательством о ПДн.

Работник: физическое лицо, вступившее в трудовые отношения с Компанией.

Смешанная обработка ПДн: обработка ПДн, включающая в себя как автоматизированную, так и неавтоматизированную обработку ПДн.

Субъект ПДн: физическое лицо, чьи ПДн обрабатываются Компанией в соответствии с настоящей Политикой, и которое прямо или косвенно определено или может быть определено с помощью обрабатываемых ПДн.

Трансграничная передача ПДн: передача ПДн на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

ПРИЛОЖЕНИЕ 2. ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

ВНД: внутренний нормативный документ.
ИСПДн: информационная система персональных данных.
ПДн: персональные данные.
РД: распорядительный документ.
РФ: Российская Федерация.

ПРИЛОЖЕНИЕ 3. ПЕРЕЧЕНЬ НОРМАТИВНЫХ ДОКУМЕНТОВ И ФОРМ

От 12.12.1993	Конституция Российской Федерации
№ 152-ФЗ от 27.07.2006	Федеральный закон «О персональных данных»
№ 149-ФЗ от 27 июля 2006	Федеральный закон «Об информации, информационных технологиях и о защите информации»
№ 160-ФЗ от 19.12.2005	Федеральный закон «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных»
№ 197-ФЗ от 30.12.2001	Трудовой кодекс Российской Федерации
№ 687 от 15.09. 2008	Постановление Правительства РФ «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»
№ 2016/679 от 27.04.2016 (принят в г. Брюсселе)	Регламент Европейского парламента и Совета Европейского Союза «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС (Общий Регламент о защите персональных данных)»