Утверждаю
Генеральный директор АО «Сбербанк-АСТ»
_____ Н.Ю. Андреев
«23» 09 2026 г.

ПОЛИТИКА В ОТНОШЕНИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В АО «СБЕРБАНК-АСТ»

ОГЛАВЛЕНИЕ

1	Обозначения и сокращения	3
2	Термины и определения	3
3	Общие положения	5
4	Цели обработки персональных данных	9
5	Правовые основания обработки персональных данных	10
6	Объем и категории обрабатываемых персональных данных	11
7	Категории субъектов персональных данных	12
8	Случаи обработки персональных данных оператором	23
9.	Согласие субъекта персональных данных на обработку его персональных данных	24
10	Порядок и условия обработки персональных данных	26
11	Особенности организации обработки персональных данных, осуществляемой без использования средств автоматизации	29
12	Актуализация, исправление, удаление и уничтожение персональных данных, ответы на запросы субъектов на доступ к персональным данным	31
13	Меры, направленные на обеспечение выполнения оператором своих обязанностей, предусмотренных Федеральным законом от 27.07.2006 N 152-ФЗ "О персональных данных"	34
14	Меры по обеспечению безопасности персональных данных при их обработке	35
15	Внутренний контроль	37
16	Перечень ссылочных документов	38
17	Приложение 1. Порядок реагирования на обращения и запросы по вопросам обработки персональных данных в АО «Сбербанк-АСТ»	40
18	Приложение 2. Форма запроса о предоставлении третьим лицом, которому поручена обработка ПДн, документов и иной информации, подтверждающих принятие мер и соблюдение в целях исполнения поручения, установленных в соответствии с ч. 3 ст. 6 Закона №152-ФЗ.	45
19	Приложение 3. Порядок оценки соблюдения третьим лицом, которому поручена обработка ПДн, конфиденциальности и обеспечения безопасности ПДн при их обработке	46
20	Приложение 4. Типовая форма поручения обработки ПДн, в том числе содержащая сроки уведомления третьим лицом, которому поручена обработка ПДн, об инцидентах, повлекших неправомерную или случайную передачу (предоставление, распространение, доступ) ПДн.	47
21	Приложение 5. Типовая форма уведомления оператора об инцидентах, повлекших неправомерную или случайную передачу (предоставление, распространение, доступ) ПДн.	48

1. ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АС – автоматизированная система.
ВНД – внутренний документ.
ИБ – информационная безопасность.
ИС – информационная система.
ИСПДн – информационная система ПДн.
ОРД – организационно-распорядительный документ.
ПДн – персональные данные.
ПФР – Пенсионный фонд России.
СОИБ – система обеспечения информационной безопасности.
ФЗ – федеральное законодательство (федеральный закон).

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Автоматизированная обработка персональных данных - обработка ПДн с помощью средств вычислительной техники ([1], ст.3, ч.4).

Биометрические персональные данные - сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются оператором для установления личности субъекта ПДн ([1], ст.11, ч.1).

Блокирование персональных данных - временное прекращение обработки ПДн работников (за исключением случаев, если обработка необходима для уточнения ПДн) ([1], ст.3, ч.7).

Информационная система персональных данных - совокупность содержащихся в базах данных ПДн и обеспечивающих их обработку информационных технологий и технических средств ([1], ст.3, ч.10).

Лицо, ответственное за организацию обработки персональных данных - работник Оператора, назначенный в соответствии с [1], ст.22.1. (получает указания непосредственно от генерального директора, и подотчетно ему) и имеющий, в частности, обязанности:

- осуществлять внутренний контроль за соблюдением оператором и его работниками законодательства Российской Федерации о ПДн, в том числе требований к защите ПДн;
- доводить до сведения работников оператора положения законодательства Российской Федерации о ПДн, локальных актов по вопросам обработки ПДн, требований к защите ПДн;
- организовывать прием и обработку обращений и запросов субъектов ПДн или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

Помимо данного лица, ответственного за организацию обработки ПДн в Обществе в целом, могут быть назначены и другие лица, ответственные за организацию обработки ПДн на отдельных направлениях работы (в отдельных подразделениях).

Обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность ПДн конкретному субъекту ПДн ([1], ст.3, ч.9).

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 ПДн ([1], ст.3, ч.3).

Обработка персональных данных без использования средств автоматизации (неавтоматизированная) - если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение ПДн в отношении каждого из субъектов ПДн, осуществляются при непосредственном участии человека ([4], ч.1).

Общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта ПДн или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности;

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 персональными данными. В данном документе Оператор - Акционерное общество «Сбербанк-Автоматизированная система торгов» (АО «Сбербанк-АСТ»).

Передача персональных данных - распространение, предоставление, доступ к персональным данным ([1], ст.3, ч.3).

Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту ПДн) ([1], ст.3, ч.1).

Персональные данные, разрешенные субъектом персональных данных для распространения, - персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом ПДн путем дачи согласия на обработку ПДн, разрешенных субъектом ПДн для распространения в порядке, предусмотренном настоящим Федеральным законом ([1], ст.3, ч.1.1).

Предоставление персональных данных - действия, направленные на раскрытие ПДн определенному лицу или определенному кругу лиц ([1], ст.3, ч.6).

Распространение персональных данных - действия, направленные на раскрытие ПДн неопределенному кругу лиц ([1], ст.3, ч.5).

Специальные категории персональных данных – персональные данные, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни ([1], ст.10, ч.1).

Уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание ПДн в информационной системе ПДн и (или) в результате которых уничтожаются материальные носители ПДн ([1], ст.3, ч.8).

Угрозы безопасности персональных данных - совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к ПДн, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение ПДн, а также иные неправомерные действия при их обработке в ИСПДн ([1], ст.19, ч.11).

Уровень защищенности персональных данных - комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности ПДн при их обработке в ИСПДн ([1], ст.19, ч.11)..

Трансграничная передача персональных данных - передача ПДн на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу ([1], ст.3, ч.11).

3. ОБЩИЕ ПОЛОЖЕНИЯ

3.1.Назначение политики

Настоящая Политика - внутренний документ АО «Сбербанк-АСТ» (далее Оператор), разработана в соответствии с требованиями [1], ст.18.1 ч.1, п.2, ч.2) и является частной политикой информационной безопасности Оператора в области обеспечения безопасности персональных данных (ПДн).

Политика определяет цели, содержание и основные направления деятельности по обеспечению законности и безопасности обработки ПДн и является основой для разработки Оператором внутренних документов (ВНД) нижнего уровня, регламентирующих процедуры обработки ПДн (положений, инструкций, стандартов и т.п.).

Содержание Политики подготовлено в соответствии с [14].

3.2.Область применения

3.2.1. Действие Политики распространяется на все информационные системы ПДн (ИСПДн) Оператора и процессы обработки ПДн.

3.2.2. В части обеспечения защиты ПДн в ИСПДн работники Оператора помимо настоящего Положения руководствуются комплектом ВНД Оператора по информационной безопасности (ИБ).

3.2.3. Во всех случаях, не урегулированных настоящим документом, а также другими ВНД и ОРД Оператор руководствуется действующим законодательством Российской Федерации.

3.2.4. Документ подлежит доведению до всех работников Общества и исполнению ими в части их касающейся ([1], ст.18.1, ч.1, п.6, ст.22.1, ч.4, п.2).

3.2.5. Доступ к документу не ограничен, документ подлежит распространению (публикации) на всех публичных Интернет-ресурсах, принадлежащих Оператору, в том числе на страницах принадлежащего оператору сайта в информационно-телекоммуникационной сети "Интернет", с использованием которых осуществляется сбор персональных данных ([1], ст.18.1, ч.2).

3.3.Права субъектов персональных данных

3.3.1. Субъект ПДн имеет право на получение информации, касающейся обработки его ПДн, в том числе содержащей ([1], ст.14, ч.7).:

- подтверждение факта обработки ПДн оператором;
- правовые основания и цели обработки ПДн;
- цели и применяемые оператором способы обработки ПДн;
- наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;

- обрабатываемые персональные данные, относящиеся к соответствующему субъекту ПДн, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- сроки обработки ПДн, в том числе сроки их хранения;
- порядок осуществления субъектом ПДн прав, предусмотренных настоящим Федеральным законом;
- информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению оператора, если обработка поручена или будет поручена такому лицу;
- информацию о способах исполнения оператором обязанностей, установленных статьей 18.1 [1];
- иные сведения, предусмотренные [1] или другими ФЗ.

3.3.2. Сведения, указанные выше, должны быть предоставлены субъекту ПДн оператором в доступной форме, и в них не должны содержаться ПДн, относящиеся к другим субъектам ПДн, за исключением случаев, если имеются законные основания для раскрытия таких ПДн ([1], ст.14, ч.2).

3.3.3. Сведения, указанные выше, предоставляются субъекту ПДн или его представителю оператором в течение десяти рабочих дней с момента обращения либо получения оператором запроса субъекта ПДн или его представителя. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления оператором в адрес субъекта ПДн мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта ПДн или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта ПДн в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки ПДн оператором, подпись субъекта ПДн или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством РФ. Оператор предоставляет сведения субъекту персональных данных или его представителю в той форме, в которой направлены соответствующие обращение либо запрос, если иное не указано в обращении или запросе ([1], ст.14, ч.3).

3.3.4. Субъект ПДн вправе запросить у Оператора указанную в предыдущем пункте информацию повторно не ранее, чем через 30 дней после первоначального обращения, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн ([1], ст. 14, ч.4). Субъект ПДн вправе запросить у Оператора указанную в предыдущем пункте информацию повторно ранее, чем через 30 дней после первоначального обращения, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения ([1], ст. 14, ч.5).

3.3.5. Субъект ПДн вправе требовать от оператора уточнения его ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав ([1], ст.14, ч.1).

3.3.6. В согласии на обработку ПДн, разрешенных субъектом ПДн для распространения, субъект ПДн вправе установить запреты на передачу (кроме

предоставления доступа) этих ПДн оператором неограниченному кругу лиц, а также запреты на обработку или условия обработки (кроме получения доступа) этих ПДн неограниченным кругом лиц ([1], ст.10.1, ч.9). Однако распространение ПДн на основании такого «согласия» Оператор не производит ([1], ст.10.1, ч.5).

3.3.7. Субъект ПДн вправе обратиться с требованием прекратить передачу (распространение, предоставление, доступ) своих ПДн, ранее разрешенных субъектом ПДн для распространения, к любому лицу, обрабатывающему его персональные данные, в случае несоблюдения положений ст.10.1 [1] или обратиться с таким требованием в суд. Данное лицо обязано прекратить передачу (распространение, предоставление, доступ) ПДн в течение трех рабочих дней с момента получения требования субъекта ПДн или в срок, указанный во вступившем в законную силу решении суда, а если такой срок в решении суда не указан, то в течение трех рабочих дней с момента вступления решения суда в законную силу.

3.3.8. Если субъект ПДн считает, что Оператор осуществляет обработку его ПДн с нарушением требований [1] или иным образом нарушает его права и свободы, субъект ПДн вправе обжаловать действия или бездействие Оператора в уполномоченный орган по защите прав субъектов ПДн или в судебном порядке ([1], ст.17, ч.1)..

3.3.9. 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 ([1], ст.17, ч.2).

3.4. **Права и обязанности Оператора персональных данных**

3.4.0. Оператор до начала обработки ПДн обязан уведомить уполномоченный орган по защите прав субъектов ПДн о своем намерении осуществлять обработку персональных данных ([1], ст.22, ч.1) , за исключением обработки ПДн ([1], ст.22, ч.2):

- включенных в государственные информационные системы ПДн, созданные в целях защиты безопасности государства и общественного порядка;
- в случае, если оператор осуществляет деятельность по обработке ПДн исключительно без использования средств автоматизации (см.п.11.1).

В случае изменения сведений, указанных оператором в уведомлении уполномоченного органа по защите прав субъектов ПДн об обработке ПДн», оператор не позднее 15-го числа месяца, следующего за месяцем, в котором возникли такие изменения, обязан уведомить уполномоченный орган по защите прав субъектов ПДн обо всех произошедших за указанный период изменениях. В случае прекращения обработки ПДн оператор обязан уведомить об этом уполномоченный орган по защите прав субъектов ПДн в течение десяти рабочих дней с даты прекращения обработки ПДн ([1], ст.22, ч.7).

Оператор обязан предоставлять лицу, ответственному за организацию обработки ПДн, сведения, указанные в ч.3, ст.22 [1].

3.4.1. Оператор, получивший доступ к ПДн, обязан соблюдать конфиденциальность ПДн - не раскрывать третьим лицам и не распространять ПДн без согласия субъекта ПДн, если иное не предусмотрено федеральным законом ([1], ст.7).

3.4.2. При сборе ПДн Оператор обязан предоставить субъекту ПДн по его просьбе информацию, предусмотренную [1], ст.14, ч. 7 ([1], ст.18, ч.1).

3.4.3. Если в соответствии с ФЗ предоставление ПДн и (или) получение оператором согласия на обработку ПДн являются обязательными, оператор обязан разъяснить субъекту персональных данных юридические последствия отказа предоставить его ПДн и (или) дать согласие на их обработку ([1], ст.18, ч.2).

3.4.4. Если ПДн получены не от субъекта ПДн, оператор, за исключением случаев, предусмотренных [1], ст. 18, ч.4, до начала обработки таких ПДн обязан предоставить субъекту ПДн следующую информацию ([1], ст.18, ч.3):

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

- цель обработки ПДн и ее правовое основание;
- перечень ПДн;
- предполагаемые пользователи ПДн;
- установленные [1] права субъекта ПДн;
- источник получения ПДн.

Оператор освобождается от обязанности предоставить субъекту ПДн эти сведения, в случаях, если ([1], ст.18, ч.4):

• субъект Пдн уведомлен об осуществлении обработки его ПДн соответствующим оператором;

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

- обработка ПДн, разрешенных субъектом ПДн для распространения, осуществляется с соблюдением запретов и условий, предусмотренных ст. 10.1 [1];
- оператор осуществляет обработку ПДн для статистических или иных исследовательских целей, для осуществления профессиональной деятельности журналиста либо научной, литературной или иной творческой деятельности, если при этом не нарушаются права и законные интересы субъекта ПДн;
- предоставление субъекту ПДн вышеуказанных сведений нарушает права и законные интересы третьих лиц.

3.4.5. Оператор обязан представить доказательства обоснованности отказа в выполнении повторного запроса субъекта ПДн ([1], ст.14, ч.6).

3.4.6. При сборе ПДн, в том числе посредством информационно-телекоммуникационной сети "Интернет", оператор обязан обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение ПДн граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, указанных в п. 2, 3, 4, 8 ч. 1 ст. 6 [1] ([1], ст.18, ч.5)..

3.4.7. Если обработка ПДн производится для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем, то заключаемый с субъектом персональных данных договор не может содержать положения, ограничивающие права и свободы субъекта персональных данных, устанавливающие случаи обработки персональных данных несовершеннолетних, если иное не предусмотрено законодательством Российской Федерации, а также положения, допускающие в качестве условия заключения договора бездействие субъекта персональных данных ([1], ст.6, ч.1, п.5).

3.4.8. Оператор обязан предоставить доказательство получения согласия субъекта ПДн на обработку его ПДн или доказательство наличия оснований, указанных в [1] в п. 2 - 11 ч. 1 ст. 6, ч. 2 ст.10 и ч. 2 ст. 11 ([1], ст.9, ч.3).

3.4.9. Оператор обязан в срок не позднее трех рабочих дней с момента получения соответствующего согласия субъекта ПДн опубликовать информацию об условиях обработки и о наличии запретов и условий на обработку неограниченным кругом лиц ПДн, разрешенных субъектом ПДн для распространения ([1], ст.10.1, ч.10).

3.4.10. Оператор ПДн вправе:

• продолжить обработку ПДн без согласия субъекта ПДн (в случае отзыва субъектом ПДн согласия на обработку ПДн) при наличии оснований, указанных в [1] в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 ([1], ст.9, ч.2).

• распространять ПДн субъекта ПДн в случае, если из предоставленного субъектом ПДн согласия на обработку ПДн, разрешенных субъектом ПДн для распространения, следует, что субъект ПДн согласился с распространением ПДн ([1], ст.10.1, ч.4), не установил запреты и условия распространения ПДн ([1], ст.10.1, ч.5, ч.9), при условии предоставления субъектом ПДн своего согласия на обработку ПДн непосредственно Оператору, либо с использованием ИС Роскомнадзора ([1], ст.10.1, ч.6);

• производить повторное распространение (или иную обработку) ПДн в некоммерческих целях (новостная или научная информация) в случае их распространения самим субъектом ПДн без предоставления Оператору согласия на распространение ПДн при наличии доказательств законности последующего распространения (или иной обработки) таких персональных данных ([1], ст.10.1, ч.2). Таким доказательством может быть ссылка на первоисточник и условия обработки запретов и ограничений на обработку неограниченным кругом лиц персональных данных, разрешенных субъектом персональных данных для распространения, установленные в первоисточнике (при их наличии, см. п.3.4.9).

▪ отказать субъекту ПДн в выполнении повторного запроса, не соответствующего условиям, предусмотренным [1], ст.14, ч.4 и 5. Такой отказ должен быть мотивированным ([1], ст.14, ч.6);

• отстаивать свои интересы в суде;

• предоставлять персональные данные субъектов третьим лицам, если это предусмотрено действующим законодательством (налоговые, правоохранительные органы и др.);

• отказывать в предоставлении ПДн в случаях, предусмотренных законодательством;

• обрабатывать персональные данные субъекта без его согласия в случаях, предусмотренных законодательством.

4. ЦЕЛИ ОБРАБОТКИ ПЕРСОНАЛЬНЬНЫХ ДАННЫХ

Обработка ПДн ограничивается достижением конкретных, заранее определенных и законных целей. Не допускается обработка ПДн, несовместимая с целями сбора ПДн.

Цели обработки ПДн происходят в том числе из анализа правовых актов, регламентирующих деятельность оператора, целей фактически осуществляемой оператором деятельности, а также деятельности, которая предусмотрена учредительными документами оператора, и конкретных бизнес-процессов оператора в конкретных информационных системах ПДн (по структурным подразделениям оператора и их процедурам в отношении определенных категорий субъектов ПДн).

Оператор производит обработку ПДн с целями:

- ведение кадрового и бухгалтерского учета;
- обеспечение соблюдения трудового законодательства РФ;
- обеспечение соблюдения налогового законодательства РФ;
- обеспечение соблюдения пенсионного законодательства РФ;
- обеспечение соблюдения законодательства о государственной социальной помощи РФ;
- обеспечение соблюдения страхового законодательства РФ;
- обеспечение соблюдения законодательства РФ о противодействии коррупции;
- обеспечение соблюдения законодательства РФ об обороне;
- подготовка, заключение и исполнение гражданско-правового договора;
- добровольное медицинское страхование;
- продвижение товаров, работ, услуг на рынке;

- обеспечение пропускного режима на территорию оператора;
- подбор персонала (соискателей) на вакантные должности оператора;
- обеспечение прохождения ознакомительной, производственной или преддипломной практики на основании договора с учебным заведением;
- реализации установленных 63-ФЗ от 06.04.2011 г. «Об электронной подписи» функций аккредитованного удостоверяющего центра;
- обеспечения проведения процедур в электронной форме на электронной площадке: государственные и муниципальные закупки, корпоративные и коммерческие закупки, продажа имущества должников- банкротов, продажа государственного, муниципального, коммерческого имущества, имущества, обращенного в собственность государства, аренда имущества, переход прав;
- предоставление дополнительных сервисов, связанных с работой на электронной площадке, в том числе: выполнение функций оператора защищенного электронного документооборота. технической поддержки клиентов;
- обеспечение доступа субъектов персональных данных к сайтам Оператора в информационно-телекоммуникационной сети "Интернет";
- обучение работе на электронной площадке;
- осуществление научной, литературной или иной творческой деятельности;
- исполнение судебного акта;
- участие в конституционном, гражданском, административном, уголовном судопроизводстве, судопроизводстве в арбитражных судах;
- осуществления прав и законных интересов оператора или третьих лиц;
- публикация новостей Оператора;
- взаимодействие с государственными органами;
- проведение проверочных мероприятий и подготовка экспертных мнений Подразделения внутренней безопасности Сбербанка в отношении Субъектов персональных данных для самостоятельного принятия Компанией мер по реагированию на риски внутреннего мошенничества;
- обеспечение информационной безопасности, в том числе безопасности ПДн при их обработке;
- аудит;
- прием посетителей и обращений.

5. ПРАВОВЫЕ ОСНОВАНИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. Обработка ПДн необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей, а именно:

- Федеральный закон №44-ФЗ от 05.04.2013 г. «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд».
- Федеральный закон №223-ФЗ от 18.07.2011г. «О закупках товаров, работ, услуг отдельными видами юридических лиц».
- Федеральный закон № 127-ФЗ от 26.10.2002 г. «О несостоятельности (банкротстве)».
- Федеральный закон № 178-ФЗ от 21.12.2001 г. «О приватизации государственного и муниципального имущества».
- Федеральный закон от 26.07.2006 № 135-ФЗ «О защите конкуренции».
- Федеральный закон от 02.10.2007 № 229-ФЗ «Об исполнительном производстве».

- Федеральный закон от 24.06.1998 № 89-ФЗ «Об отходах производства и потребления».
- Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи».
- Федеральный закон от 28.03.1998 г. N 53-ФЗ "О воинской обязанности и военной службе".
- Федеральный закон от 25 декабря 2008 г. N 273-ФЗ "О противодействии коррупции".
- Федеральный закон от 30 декабря 2008 г. N 307-ФЗ "Об аудиторской деятельности".
- Федеральный закон от 27 июля 2006 г. N 152-ФЗ "О персональных данных", ст. 18.1 и 19.
- Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации", ст. 16, ч. 4.
- Гражданский кодекс.
- Жилищный кодекс.
- Лесной кодекс.
- Земельный кодекс.
- Трудовой кодекс.
- Налоговый кодекс.

5.2. Обработка ПДн необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем.

Примечание:

Заключаемый с субъектом персональных данных договор не может содержать положения, ограничивающие права и свободы субъекта персональных данных.

5.3. Обработка ПДн осуществляется с согласия субъекта персональных данных на обработку его персональных данных.

5.4. Обработка ПДн необходима для осуществления прав и законных интересов оператора или третьих лиц.

5.5. Обработка ПДн осуществляется в связи с участием лица в конституционном, гражданском, административном, уголовном судопроизводстве, судопроизводстве в арбитражных судах.

5.6. Обработка ПДн необходима для исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве.

5.7. Обработка ПДн необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта ПДн, если получение согласия субъекта ПДн невозможно.

5.8. Обработка ПДн необходима для научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и законные интересы субъекта ПДн.

5.9. Осуществляется обработка ПДн, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

6. ОБЪЕМ И КАТЕГОРИИ ОБРАБАТЫВАЕМЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. Объем обрабатываемых ПДн – более 100 000 субъектов ПДн для ИСПДн электронной площадки АС «Сбербанк-АСТ» и менее 100 000 субъектов ПДн для иных ИСПДн.

6.2. Категории обрабатываемых ПДн (согласно классификации, установленной [1] и [3]):

- общедоступные;
- специальные;
- иные.

6.3. Содержание и объем обрабатываемых ПДн должны соответствовать заявленным целям обработки, не должны быть избыточными.

7. КАТЕГОРИИ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1. Категории субъектов ПДн, согласно классификации, используемой [3]:

- не сотрудники Оператора;
- сотрудники Оператора.

7.2. Категории субъектов ПДн, согласно классификации https://pd.rkn.gov.ru/operators-registry/notification/updateform/ :

- работники;
- соискатели;
- родственники работников;
- уволенные работники;
- контрагенты;
- представители контрагентов;
- клиенты;
- посетители сайта;
- выгодоприобретатели по договорам;
- студенты;
- законные представители;
- иные категории (посетители и обратившиеся лица, ФЛ - представители сторон в договорах, субъекты новостей, контактные должностные лица, участники мероприятий, ФЛ - фигуранты судопроизводства).

В таблице 1 для каждой цели обработки персональных данных представлены категории и перечень обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, способы, сроки их обработки и хранения, порядок уничтожения персональных данных при достижении целей их обработки или при наступлении иных законных оснований ([1], ст.18.1, ч.1, п.2).

№	Цель обработки ПДн	Категории ПДн	Перечень обрабатываемых ПДн	Категории субъектов ПДн	Способы обработки ПДн	Сроки обработки ПДн	Сроки хранения ПДн	Порядок уничтожения ПДн
1	Ведение кадрового и бухгалтерского учета	иные; специальные,	фамилия, имя, отчество; год рождения; месяц рождения; дата рождения; место рождения; семейное положение; доходы; пол; адрес электронной почты; адрес места жительства; адрес регистрации; номер телефона; СНИЛС; ИНН; гражданство; данные документа, удостоверяющего личность; номер счета; профессия; должность; сведения о трудовой деятельности (в том числе стаж работы, данные о трудовой занятости на текущее время); отношение к воинской обязанности, сведения о воинском учете; сведения об образовании; сведения о судимости; дата регистрации по месту регистрации, сведения о квалификации, сведения о повышении квалификации, профессиональной переподготовке, знание иностранного языка, ученое звание и степень, состояние в браке, состав семьи, вид работы (основная, по совместительству), трудовая функция (работа по должности в соответствии со штатным расписанием, профессии, специальности с указанием квалификации, конкретный вид поручаемой работнику работы, табельный номер, основание прекращения трудового договора (увольнения), структурное подразделение, сведения о представителе	Работники; уволенные работники, родственники работников.	С использованием или без использования средств автоматизации	В период наличия трудовых отношений и (или) хранения учетных документов.	В соответствии с п. 10.5.	В соответствии с п.11.8 и п. 12.11.

			работодателя, подписавшем трудовой договор, и основание, в силу которого он наделен соответствующими полномочиями, условия оплаты труда, тарифная ставка (оклад, надбавка), режим рабочего времени и времени отдыха, учетные данные по рабочему времени работника, условия труда на рабочем месте, сведения об аттестации работника, сведения о наградах, поощрениях, почетных званиях, сведения об отпусках работника, сведения о социальных льготах работника, сведения о дисциплинарных взысканиях работника, сведения об инвалидности работника.					
2	Обеспечение соблюдения трудового законодательства РФ	иные; специальные.	Фамилия, имя, отчество; год рождения; месяц рождения; дата рождения; место рождения; семейное положение; доходы; пол; адрес электронной почты; адрес места жительства; адрес регистрации; номер телефона; СНИЛС; ИНН; гражданство; данные документа, удостоверяющего личность; профессия; должность; сведения о трудовой деятельности (в том числе стаж работы, данные о трудовой занятости на текущее время); отношение к воинской обязанности, сведения о воинском учете; сведения об образовании; сведения о судимости (в случаях, предусмотренных ФЗ), дата регистрации по месту регистрации, сведения о квалификации, сведения о повышении квалификации, профессиональной переподготовке, знание иностранного языка, ученое звание и степень, состояние в браке, состав семьи, вид работы (основная, по	Работники; уволенные работники; родственники работников.	С использованием или без использования средств автоматизации	В период наличия трудовых отношений и (или) хранения учетных документов.	В соответствии с п. 10.5.	В соответствии с п.11.8 и п. 12.11.

			совместительству), трудовая функция (работа по должности в соответствии со штатным расписанием, профессии, специальности с указанием квалификации, конкретный вид поручаемой работнику работы, табельный номер, основание прекращения трудового договора (увольнения), структурное подразделение, сведения о представителе работодателя, подписавшем трудовой договор, и основание, в силу которого он наделен соответствующими полномочиями, условия оплаты труда, тарифная ставка (оклад, надбавка), режим рабочего времени и времени отдыха, учетные данные по рабочему времени работника, условия труда на рабочем месте, сведения об аттестации работника, сведения о наградах, поощрениях, почетных званиях, сведения об отпусках работника, сведения о социальных льготах работника, сведения о дисциплинарных взысканиях работника, сведения об инвалидности работника.					
3	Обеспечение соблюдения налогового законодательства РФ	Иные	Фамилия, имя, отчество; доходы, адрес регистрации, СНИЛС, ИНН. Сведения о начислениях, удержаниях и выплатах денежных средств.	Работники, контрагенты – ФЛ.	С использованием или без использования средств автоматизации	В период наличия трудовых или договорных отношений и (или) хранения учетных документов.	В соответствии с п. 10.5.	В соответствии с п.11.8 и п. 12.11.
4	Обеспечение соблюдения пенсионного законодательства РФ	Иные	Фамилия, имя, отчество; год рождения; месяц рождения; дата рождения; пол; СНИЛС; гражданство. Сведения о	Работники	С использованием или без использования	В период наличия трудовых отношений и (или) хранения	В соответствии с п. 10.5.	В соответствии с п.11.8 и п. 12.11.

			начислениях, удержаниях и выплатах денежных средств.		средств автоматизации	учетных документов.		
5	Обеспечение соблюдения законодательства о государственной социальной помощи РФ	Иные	Фамилия, имя, отчество; год рождения; месяц рождения; дата рождения; семейное положение; доходы; адрес места жительства; адрес регистрации; СНИЛС; гражданство; данные документа, удостоверяющего личность; номер расчетного счета; Сведения о льготах, инвалидности, составе семьи. Сведения о начислениях и выплатах денежных средств.	Работники	С использование м или без использования средств автоматизации	В период наличия трудовых отношений и (или) хранения учетных документов.	В соответствии с п. 10.5.	В соответств ии с п.11.8 и п. 12.11.
6	Обеспечение соблюдения страхового законодательства РФ	Иные	Фамилия, имя, отчество; год рождения; месяц рождения; дата рождения; СНИЛС; гражданство; данные документа, удостоверяющего личность; номер расчетного счета. Сведения о страховых выплатах денежных срелств.	Работники	С использование м или без использования средств автоматизации	В период наличия трудовых отношений и (или) хранения учетных документов.	В соответствии с п. 10.5.	В соответств ии с п.11.8 и п. 12.11.
7	Обеспечение соблюдения законодательства РФ об обороне	Иные	Фамилия, имя, отчество; год рождения; месяц рождения; дата рождения; место рождения; семейное положение; адрес места жительства; номер телефона; данные документа, удостоверяющего личность; данные водительского удостоверения; профессия; должность; отношение к воинской обязанности, сведения о воинском учете; сведения об образовании; Семейное положение, состав семьи, знание иностранных языков.	Работники, родственник и работников.	С использование м или без использования средств автоматизации	В период наличия трудовых отношений и (или) хранения учетных документов.	В соответствии с п. 10.5.	В соответств ии с п.11.8 и п. 12.11.
8	Обеспечение соблюдения законодательства РФ о противодействии коррупции.	Иные	Фамилия, имя, отчество, место работы, должность, подразделение, бизнес-интерес, создающий конфликт интересов с работодателем, доля в уставном	Работники.	Без использования средств автоматизации	В период наличия трудовых отношений и (или) хранения	В соответствии с п. 10.5.	В соответств ии с п.11.8 и п. 12.11.

			капитале сторонних ЮЛ, внешняя работа по совместительству или договору ГПХ.			учетных документов.		
9	Подготовка, заключение и исполнение гражданско-правового договора	Иные	Фамилия, имя, отчество; год рождения; месяц рождения; дата рождения; адрес места жительства; адрес регистрации; СНИЛС; ИНН; гражданство; данные документа, удостоверяющего личность; номер расчетного счета; сведения об образовании, номер телефона, адрес электронной почты	Работники, выгодоприобретатели, ФЛ - представители сторон по договорам.	С использованием или без использования средств автоматизации	В период наличия договорных отношений и (или) хранения учетных документов.	В соответствии с п. 10.5.	В соответствии с п.11.8 и п. 12.11.
10	Добровольное медицинское страхование	Иные	Фамилия, имя, отчество; год рождения; месяц рождения; дата рождения; пол; адрес места жительства; адрес регистрации; номер телефона; СНИЛС; данные документа, удостоверяющего личность;	Работники	С использованием или без использования средств автоматизации	В период действия согласия на обработку Пдн с данной целью.	В период действия согласия на обработку Пдн с данной целью.	В соответствии с п.11.8 и п. 12.11.
11	Продвижение товаров, работ, услуг на рынке	Иные	Адрес электронной почты; номер телефона. Статистика посещений страниц сайта и операций (в том числе собираемая с использованием метрических программ Яндекс-Метрика).	Клиенты, посетители сайта.	Без использования средств автоматизации	В период действия согласия на обработку ПДн с данной целью.	В период действия согласия на обработку Пдн с данной целью.	В соответствии с п.11.8 и п. 12.11.
		Общедоступные	Фамилия, имя, отчество, должность, ученая степень, ученое звание, место работы, публикации, контактный телефон и адрес электронной почты, личное фото (не в целях идентификации личности).	Работники.	Без использования средствавтоматизации	В период действия согласия на обработку ПДн с данной целью.	В период действия согласия на обработку Пдн с данной целью.	В соответствии с п.11.8 и п. 12.11.
12	Обеспечение пропускного режима на территорию оператора	Иные	Фамилия, имя, отчество; данные документа, удостоверяющего личность.	Работники; Соискатели; Уволенные работники; Контрагенты; Представители контрагентов; Клиенты;	Без использования средств автоматизации	В период приема посетителя.	3 года.	В соответствии с п.11.8 и п. 12.11.

				Студенты; Законные представители и Посетители.				
13	Подбор персонала (соискателей) на вакантные должности оператора	Иные, специальные	Фамилия, имя, отчество; год рождения; пол; адрес электронной почты; адрес места жительства; адрес регистрации; номер телефона; гражданство; профессия; сведения о трудовой деятельности (в том числе стаж работы, данные о трудовой занятости на текущее время с указанием наименования и расчетного счета организации); сведения об образовании; сведения о судимости (в случаях, установленных ФЗ); Сведения о повышении квалификации	Соискатели	Без использования средств автоматизации	В период соискания.	Не хранятся	В соответствии с п.11.8 и п. 12.11.
14	Обеспечение прохождения ознакомительной, производственной или преддипломной практики на основании договора с учебным заведением	Иные	Фамилия, имя, отчество; год рождения; адрес места жительства; адрес регистрации; данные документа, удостоверяющего личность; профессия; сведения о трудовой деятельности (в том числе стаж работы, данные о трудовой занятости на текущее время; сведения об образовании;	Студенты	Без использования средств автоматизации	В период соискания.	В соответствии с п. 10.5.	В соответствии с п.11.8 и п. 12.11.
15	Реализации установленных 63-ФЗ от 06.04.2011 г. «Об электронной подписи» функций аккредитованного удостоверяющего центра.	Иные	Фамилия, имя, отчество; год рождения; месяц рождения; дата рождения; место рождения; адрес электронной почты; адрес места жительства; адрес регистрации; номер телефона; СНИЛС; ИНН; данные документа, удостоверяющего личность; должность; наименование подразделения.	Работники, клиенты	С использованием или без использования средств автоматизации	В период существования аккредитованного УЦ.	В период существования аккредитованного УЦ.	Не уничтожаются. Передаются в Минкомсвязь в соответствии с 63-ФЗ 2022 г.

16	Обеспечение проведения процедур в электронной форме на электронной площадке: государственные и муниципальные закупки, корпоративные и коммерческие закупки, продажа имущества должников- банкротов, продажа государственного, муниципального, коммерческого имущества, имущества, обращенного в собственность государства, аренда имущества, переход прав.	Иные, Специальные, общедоступные.	Фамилия, имя, отчество; год рождения; месяц рождения; дата рождения; адрес электронной почты; адрес места жительства; адрес регистрации; номер телефона; СНИЛС; ИНН; данные документа, удостоверяющего личность; данные документа, удостоверяющего личность за пределами Российской Федерации; номер расчетного счета; должность; сведения о судимости – в случаях, предусмотренных ФЗ; место работы; иные ПДн, которые клиенты могут загрузить в ИСПДн в составе своих документов.	Клиенты, работники.	С использованием или без использования средств автоматизации	В период регистрации на электронной площадке	10 лет в случае КЭП и 5 лет в остальных случаях (см. п. 10.5)	В соответствии с п.11.8 и п. 12.11.
17	Предоставление дополнительных сервисов, связанных с работой на электронной площадке;выполнение функций оператора защищенного электронного документооборота	Иные	Фамилия, имя, отчество; СНИЛС; ИНН; данные документа, удостоверяющего личность; иные ПДн, которые клиенты могут загрузить в ИСПДн в составе своих документов.	Клиенты.	С использованием или без использования средств автоматизации	В период регистрации на электронной площадке	В период действия согласия на обработку Пдн с данной целью.	В соответствии с п.11.8 и п. 12.11.
18	Обеспечение доступа субъектов персональных данных к сайтам Оператора в информационно-телекоммуникационной сети "Интернет".	Иные	Имя учетной записи (логин), пароль, сертификат ключа проверки электронной подписи, уникальные внутренние идентификаторы (ID).	Клиенты, работники.	С использованием средств автоматизации.	В период регистрации на сайте	В соответствии с п. 10.5.	В соответствии с п.11.8 и п. 12.11.
			Содержимое Интернет-трафика, HTTP(HTTPS)- запросов к сайту и ответов на них, включая HTTP-заголовки,		С использование	В период HTTP (HTTPS) – сеанса.	Не хранятся (за исключением	Нет хранения – нет и

			в том числе: IP-адреса, User-Agent, Cookie и т.п. – в случае отнесения этой информации к ПДн.		м средств автоматизации.		ПДн, попавших в журналы регистрации событий ИБ).	уничтожения.
			ПДн, попавшие в журналы регистрации событий информационной безопасности.		С использованием или без использования средств автоматизации	Равен сроку хранения журналов регистрации событий информационной безопасности	Равен сроку хранения журналов регистрации событий информационной безопасности.	Автоматически, в соответствии с функционалом средств журналирования.
19	Обучение работе на электронной площадке	Иные	Фамилия, имя, отчество; адрес электронной почты; номер телефона; данные документа, удостоверяющего личность; Организация (место работы)	Клиенты, выгодоприобретатели по договорам.	С использованием или без использования средств автоматизации	В период регистрации на учебном сайте.	В соответствии с п. 10.5.	В соответствии с п.11.8 и п. 12.11.
20	Прием посетителей и обращений	Иные.	Фамилия, имя, отчество; адрес электронной почты; адрес места жительства; адрес регистрации; номер телефона; данные документа, удостоверяющего личность; иные ПДн, которые могут быть в обращении.	Субъекты персональных данных, обратившиеся с различными вопросами и требованиями.	С использованием или без использования средств автоматизации	В соответствии с п. 10.5.	В соответствии с п. 10.5.	В соответствии с п.11.8 и п. 12.11.
21	Публикация новостей Оператора.	Общедоступные.	Фамилия, имя, отчество, должность, место работы.	Субъекты новостей, персональные данные которых публичны.	Без использования средств автоматизации.	В течение периода публикации новости на сайте Оператора.	Нет.	В соответствии с п.11.8 и п. 12.11, - если возникло основание для

								уничтожения ПДн.
22	Осуществление прав и законных интересов Оператора или третьих лиц.	Иные	Фамилия, имя, отчество, должность, место работы, контактный номер телефона и eMail, данные документа, удостоверяющего личность, сумма долга или ущерба..	Работники, клиенты, контрагенты	Без использования средств автоматизации.	В период реализации прав (законных интересов).	В течение сроков исковой давности.	В соответствии с п.11.8 и п. 12.11, - если возникло основание для уничтожения ПДн.
23	Взаимодействие с государственными органами	Иные	Фамилия, имя, отчество, должность, место работы, контактный номер телефона и eMail.	Контактные должностные лица	Без использования средств автоматизации.	В период взаимодействия.	Нет.	В соответствии с п.11.8 и п. 12.11, - если возникло основание для уничтожения ПДн.
24	Осуществление научной, литературной или иной творческой деятельности;	Иные	Фамилия, имя, отчество, должность, место работы, ученая степень, контактный номер телефона и eMail.	Участники мероприятий.	Без использования средств автоматизации.	В период подготовки и проведения мероприятия.	В соответствии с п. 10.5.	В соответствии с п.11.8 и п. 12.11.
25	Исполнение судебного акта;	Иные	ПДн, указанные в судебном акте.	ФЛ - фигуранты судебного акта.	Без использования средств автоматизации.	В период подготовки и проведения мероприятия.	В соответствии с п. 10.5.	В соответствии с п.11.8 и п. 12.11.
26	Участие в конституционном, гражданском, административном, уголовном судопроизводстве,	Иные	ПДн, фигурантов и участников, указанные в материалах дела.	ФЛ - фигуранты и участники.	Без использования средств автоматизации.	В период подготовки и проведения судопроизводства.	В соответствии с п. 10.5.	В соответствии с п.11.8 и п. 12.11.

	судопроизводстве в арбитражных судах.							
27	Проведение проверочных мероприятий и подготовка экспертных мнений Подразделения внутренней безопасности Сбербанка в отношении Субъектов персональных данных для самостоятельного принятия Компанией мер по реагированию на риски внутреннего мошенничества	Иные	фамилия, имя, отчество, дата рождения, место рождения, адрес электронной почты, адрес места жительства, адрес регистрации, номер телефона, гражданство, данные документа, удостоверяющего личность, профессия, должность, сведения о трудовой деятельности (в том числе стаж работы, данные о трудовой занятости на текущее время с указанием наименования и расчетного счета организации), сведения об образовании; информация об изменении ФИО, наличие второго (иного) гражданства,	Работники, соискатели, родственники и работников.	Без использования средств автоматизации.	В период проведения проверочных мероприятий.	В соответствии с п. 10.5.	В соответствии с п.11.8 и п. 12.11.
28	Обеспечение информационной безопасности, в том числе безопасности ПДн при их обработке.	Иные	Весь перечень обрабатываемых ПДн.	Весь перечень субъектов ПДн,	С использованием или без использования средств автоматизации.	В период обработки ПДн в ИС	В соответствии с п. 10.5.	В соответствии с п.11.8 и п. 12.11.
29	Аудит	Иные	фамилия, имя, отчество, адрес электронной почты, номер телефона, данные документа, удостоверяющего личность, должность, сведения о трудовой деятельности, номер счета, суммы зачислений, удержаний, выплат.	Работники, бывшие работники, родственники и работников.	С использованием или без использования средств автоматизации.	В период проведения аудита	В соответствии с п. 10.5.	В соответствии с п.11.8 и п. 12.11.

Таблица 1.

8. СЛУЧАИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ ОПЕРАТОРОМ

Обработка Оператором ПДн осуществляется в следующих случаях, установленных [1], ст.6, ч.1:

- обработка ПДн осуществляется с согласия субъекта ПДн на обработку его ПДн ([1], ст.6,ч.1, п.1);
- обработка ПДн необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей ([1], ст.6, ч.1, п.2);
- обработка ПДн осуществляется в связи с участием лица в конституционном, гражданском, административном, уголовном судопроизводстве, судопроизводстве в арбитражных судах ([1], ст.6, ч.1, п.3);
- обработка ПДн необходима для исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве ([1], ст.6, ч.1, п.3.1);
- обработка ПДн необходима 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 ([1], ст.6, ч.1, п.5);
- обработка ПДн необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта ПДн, если получение согласия субъекта ПДн невозможно ([1], ст.6, ч.1, п.6);
- обработка ПДн необходима для осуществления прав и законных интересов оператора или третьих лиц, в том числе в случаях, предусмотренных Федеральным законом "О защите прав и законных интересов физических лиц при осуществлении деятельности по возврату просроченной задолженности и о внесении изменений в Федеральный закон "О микрофинансовой деятельности и микрофинансовых организациях", либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта ПДн ([1], ст.6, ч.1, п.7);
- обработка ПДн необходима для научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и законные интересы субъекта ПДн ([1], ст.6, ч.1, п.8);
- осуществляется обработка ПДн, подлежащих опубликованию или обязательному раскрытию в соответствии с ФЗ ([1], ст.6, ч.1, п.11).

Обработка ПДн сотрудников органов федеральной службы безопасности, подлежащих государственной защите судей, должностных лиц правоохранительных и контролирующих органов, подлежащих государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства, сотрудников органов внутренних дел, лиц, оказывающих или оказывавших им содействие на конфиденциальной основе, осуществляется с учетом особенностей, предусмотренных [1], ст.6, ч.1.2.

Сторонами, участвующими в обработке ПДн, являются ([15], п.5.1):

- субъект ПДн;
- оператор ПДн (в том числе другие операторы ПДн);
- обработчик ПДн – в случае, если оператор персональных данных поручает обработку ПДн или сам является обработчиком ПДн в отношении другого оператора ПДн.

9. СОГЛАСИЕ СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ НА ОБРАБОТКУ ЕГО ПЕРСОНАЛЬНЫХ ДАННЫХ

9.1. Субъект ПДн принимает решение о предоставлении его ПДн и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку персональных данных должно быть конкретным, предметным, информированным, сознательным и однозначным. Согласие на обработку ПДн может быть дано субъектом ПДн или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом ([1], ст.9, ч.1).

Согласие на обработку персональных данных должно быть оформлено отдельно от иных информации и (или) документов, которые подтверждает и (или) подписывает субъект персональных данных ([1], ст.9, ч.1), за исключением случаев, установленных п. 11.6 ([1], ст.4, ч.3).

В случае получения согласия на обработку ПДн от представителя субъекта ПДн полномочия данного представителя на дачу согласия от имени субъекта ПДн проверяются оператором ([1], ст.9, ч.1).

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

9.3. Обязанность предоставить доказательство получения согласия субъекта ПДн на обработку его ПДн или доказательство наличия оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 [1], возлагается на оператора ([1], ст.9, ч.3).

9.4. В случаях, предусмотренных федеральным законом, обработка ПДн осуществляется только с согласия субъекта ПДн, в письменной форме установленной [1], ст.9, ч.4. Это следующие случаи:

- для передачи ПДн работника третьей стороне, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в других случаях, предусмотренных Трудовым Кодексом или иными федеральными законами ([2], ст.88);
- для включения ПДн субъекта ПДн в общедоступные источники ([1], ст.8);
- в случае обработки специальных категорий ПДн ([1], ст.10, ч.2, п.1).
- в случае обработки биометрических ПДн ([1], ст.11, ч.1);
- в случае трансграничной передачи ПДн на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов ПДн в соответствии с [1], ст.12, ч.4, п.1;
- если решение, порождающее юридические последствия в отношении субъекта ПДн или иным образом затрагивающее его права и законные интересы, может быть принято на основании исключительно автоматизированной обработки его ПДн и это не предусмотрено ФЗ ([1], ст.16, ч.2).

9.5. Равнозначным содержащему собственноручную подпись субъекта ПДн согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью ([1], ст.9, ч.4).

9.6. Согласие в письменной форме субъекта ПДн на обработку его ПДн, за исключением случаев, установленных п.9.8, п.11.6, 2-й дефис, должно включать в себя, в частности ([1], ст.9, ч.4):

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

- фамилию, имя, отчество, адрес представителя субъекта ПДн, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта ПДн);
- наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта ПДн;
- цель обработки ПДн;
- перечень ПДн, на обработку которых дается согласие субъекта ПДн;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению оператора, если обработка будет поручена такому лицу;
- перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки ПДн;
- срок, в течение которого действует согласие субъекта ПДн, а также способ его отзыва, если иное не установлено федеральным законом;
- подпись субъекта ПДн.

9.7. Согласие на обработку ПДн, разрешенных субъектом ПДн для распространения, оформляется отдельно от иных согласий субъекта ПДн на обработку его ПДн. Оператор обязан обеспечить субъекту ПДн возможность определить перечень ПДн по каждой категории ПДн, указанной в согласии на обработку ПДн, разрешенных субъектом ПДн для распространения ([1], ст.10.1, ч.1).

9.8. Согласие на обработку ПДн, разрешенных субъектом ПДн для распространения, имеет письменную форму, отличную от указанной в п. 9.6 и должно содержать следующую информацию [5]:

- фамилия, имя, отчество (при наличии) субъекта ПДн;
- контактная информация (номер телефона, адрес электронной почты или почтовый адрес субъекта ПДн);
- текст, содержащий в явном виде согласие субъекта ПДн с распространением его персональных данных ([1], ст.10.1, ч.4);
- сведения об операторе-организации - наименование, адрес, указанный в Едином государственном реестре юридических лиц, идентификационный номер налогоплательщика, основной государственный регистрационный номер (если он известен субъекту ПДн);
- сведения об операторе - физическом лице - фамилия, имя, отчество (при наличии), место жительства или место пребывания;
- сведения об операторе-гражданине, являющимся индивидуальным предпринимателем, - фамилия, имя, отчество (при наличии), идентификационный номер налогоплательщика, основной государственный регистрационный номер (если он известен субъекту ПДн);
- сведения об информационных ресурсах оператора (адрес, состоящий из наименования протокола (http или https), сервера (www), домена, имени каталога на сервере и имя файла веб-страницы), посредством которых будут осуществляться предоставление доступа неограниченному кругу лиц и иные действия с ПДн субъекта ПДн;
- цель (цели) обработки ПДн;
- категории и перечень ПДн, на обработку которых дается согласие субъекта ПДн:
- персональные данные (фамилия, имя, отчество (при наличии), год, месяц, дата рождения, место рождения, адрес, семейное положение, образование, профессия, социальное положение, доходы, другая информация, относящаяся к субъекту ПДн);
- специальные категории ПДн (расовая, национальная принадлежности, политические взгляды, религиозные или философские убеждения, состояние здоровья, интимной жизни, сведения о судимости);

- биометрические ПДн;
- категории и перечень ПДн, для обработки которых субъект ПДн устанавливает условия и запреты, а также перечень устанавливаемых условий и запретов [3] (заполняется по желанию субъекта ПДн, однако в случае заполнения Оператор не производит распространение ПДн на основании данного «согалсия» ([1], ст.10.1, ч.5));
- условия, при которых полученные ПДн могут передаваться оператором, осуществляющим обработку ПДн, только по его внутренней сети, обеспечивающей доступ к информации лишь для строго определенных сотрудников, либо с использованием информационно-телекоммуникационных сетей, либо без передачи полученных ПДн (заполняется по желанию субъекта ПДн, однако в случае заполнения Оператор не производит распространение ПДн на основании данного «согалсия» ([1], ст.10.1, ч.5)) [4];
- срок действия согласия.

9.9. Обработка ПДн в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи, а также в целях политической агитации допускается только при условии предварительного согласия субъекта ПДн. Указанная обработка ПДн признается осуществляемой без предварительного согласия субъекта ПДн, если оператор не докажет, что такое согласие было получено ([1], ст..15, ч.1).

Оператор обязан немедленно прекратить по требованию субъекта ПДн обработку его ПДн ([1], ст..15, ч.2).

Для обеспечения возможности выполнения данного требования клиента независимо от наличия других целей обработки его ПДн, согласие на обработку ПДн в целях продвижения товаров, работ, услуг должно быть оформлено отдельно от иных согласий.

10. ПОРЯДОК И УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

10.1. Оператор осуществляет обработку ПДн в случаях, указанных в разделе 8 - операции, совершаемые с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (предоставление, доступ), распространение, блокирование, удаление, уничтожение ПДн.

10.2. Обработка ПДн осуществляется с соблюдением принципов и правил, предусмотренных [1].

10.3. Обработка ПДн оператором ограничивается достижением конкретных, заранее определенных и законных целей ([1], ст.5, ч.2). Обработке подлежат только персональные данные, которые отвечают целям их обработки. Содержание и объем обрабатываемых ПДн должны соответствовать заявленным целям обработки.

10.4. Хранение ПДн должно осуществляться в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом ([1], ст.5, ч.7).

10.5. Сроки обработки (в том числе хранения) ПДн:

- Оператором электронной площадки АС «Сбербанк-АСТ» в рамках процедур, проводимых в соответствии с 44-ФЗ 2013 г., 223-ФЗ 2011 г. – не менее 10 лет ([9], п.22).

- Оператором электронной площадки АС «Сбербанк-АСТ» в рамках иных процедур, срок хранения ПДн в отношении которых ФЗ не установлен – 5 лет ([11], п.11 и 12).
- Срок хранения согласий на обработку ПДн – 3 года с момента прекращения действия согласия [11].
- Договоры, соглашения, контракты документы (акты, протоколы разногласий) к ним 5 лет ([11], п.11).
- Документы (расчеты, заключения, справки, переписка) к договорам, соглашениям, контрактам ([11], п.12).
- Личные карточки и личные дела работников, сведения о трудовой деятельности и трудовом стаже работника, в том числе в виде баз данных – 50/75 лет [11].
- Характеристики, справки об объективных сведениях на работников, Листы собеседования – 5 лет [11].
- Списки (реестры) поставщиков (подрядчиков, исполнителей) и покупателей (заказчиков) – 5 лет [11].
- Реестры выданных и аннулированных сертификатов ключей проверки электронных подписей удостоверяющих центров – в период существования удостоверяющего центра [13].
- Содержимое Интернет-трафика, HTTP(HTTPS)- запросов к сайту и ответов на них, включая HTTP-заголовки, в том числе: IP-адреса, User-Agent, Cookie и т.п.(в случае подпадания этой информации под ПДн). Срок обработки - в течение существования сеанса (сессии) HTTP(HTTPS). Данная информация не хранится, за исключением той ее части, которая попадает в журналы регистрации событий информационной безопасности.
- ПДн, попавшие в журналы регистрации событий информационной безопасности. Срок их хранения равен установленному сроку хранения журналов регистрации событий информационной безопасности.

Примечание: [11] устанавливает также сроки хранения множества других документов, содержащих персональные данные.

10.6. При осуществлении хранения ПДн оператор ПДн обязан использовать базы данных, находящиеся на территории Российской Федерации. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой ([1], ст.5, ч.3)

10.7. Условием прекращения обработки ПДн может являться достижение целей обработки ПДн, истечение срока действия согласия или отзыв согласия субъекта ПДн на обработку его ПДн, а также выявление неправомерной обработки ПДн.

10.8. Оператор вправе поручить обработку ПДн другому лицу с согласия субъекта ПДн, если иное не предусмотрено ФЗ, на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия государственным органом или муниципальным органом соответствующего акта (далее - поручение оператора). Лицо, осуществляющее обработку ПДн по поручению оператора, обязано соблюдать принципы и правила обработки ПДн, предусмотренные [1], соблюдать конфиденциальность ПДн, принимать необходимые меры, направленные на обеспечение выполнения обязанностей, предусмотренных [1]. В поручении оператора должны быть определены перечень ПДн, перечень действий (операций) с ПДн, которые будут совершаться лицом, осуществляющим обработку ПДн, цели их обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность ПДн, требования, предусмотренные частью 5 статьи 18 и статьей 18.1 [1] обязанность по запросу оператора ПДн в течение срока действия поручения оператора, в том числе до обработки персональных данных, предоставлять документы и иную информацию, подтверждающие принятие мер и соблюдение в целях исполнения поручения оператора требований, установленных в соответствии с ст.6 [1], обязанность обеспечивать безопасность ПДн при их обработке, а также должны быть указаны требования к защите обрабатываемых ПДн в

соответствии со статьей 19 [1], в том числе требование об уведомлении оператора о случаях, предусмотренных частью 3.1 статьи 21 [1] ([1], ст. 6, ч.3).

10.9. Лицо, осуществляющее обработку ПДн по поручению оператора, не обязано получать согласие субъекта ПДн на обработку его ПДн ([1], ст. 6, ч.4).

10.10. В случае, если оператор поручает обработку ПДн другому лицу, ответственность перед субъектом ПДн за действия указанного лица несет оператор. Лицо, осуществляющее обработку ПДн по поручению оператора, несет ответственность перед оператором ([1], ст. 6, ч.5). В случае, если оператор поручает обработку персональных данных иностранному физическому лицу или иностранному юридическому лицу, ответственность перед субъектом персональных данных за действия указанных лиц несет оператор и лицо, осуществляющее обработку персональных данных по поручению оператора ([1], ст. 6, ч.6).

10.11. Предоставление ПДн (или доступа к ним) третьим лицам к персональным данным может производиться Оператором только в следующих случаях:

- на основании федерального закона. В этом случае порядок предоставления ПДн регламентируется этим законом, его подзаконными актами, а также содержится в соответствующих запросах уполномоченных на это государственных органов;
- на основании договора, предусматривающего подобное представление ПДн (или доступа к ним) и при наличии согласия субъекта ПДн на предоставление ПДн (или доступа к ним) указанным третьим лицам. В этом случае порядок представления ПДн (или доступа к ним) определяется соответствующим договором. При заключении подобных договоров Оператор обязан обеспечить их соответствие требованиям федеральных законов и подзаконных актов в области обеспечения защиты ПДн.

10.12. Оператор вправе передавать персональные данные органам дознания и следствия, иным уполномоченным органам по основаниям, предусмотренным действующим законодательством Российской Федерации.

10.13. Передача (распространение, предоставление, доступ) ПДн, разрешенных субъектом ПДн для распространения, должна быть прекращена в любое время по требованию субъекта ПДн. Данное требование должно включать в себя фамилию, имя, отчество (при наличии), контактную информацию (номер телефона, адрес электронной почты или почтовый адрес) субъекта ПДн, а также перечень ПДн, обработка которых подлежит прекращению. Указанные в данном требовании персональные данные могут обрабатываться только оператором, которому оно направлено.

10.14. Оператор принимает меры предусмотренные ч. 2 ст. 18.1, ч. 1 ст. 19 152-ФЗ "О ПДн", обеспечивает защиту и конфиденциальность (в соответствии со ст. 7 152-ФЗ) обрабатываемых ПДн, а также в соответствии с требованиями нормативных документов ФСТЭК РФ и ФСБ РФ, что подтверждается аттестатом соответствия ИСПДн, подлежащих аттестации в соответствии с требованиями законодательства по обеспечению безопасности информации.

10.15. Юридические и физические лица, производящие загрузку (запись) на электронную площадку АС «Сбербанк-АСТ» ПДн (в том числе в составе загружаемых ими документов), обработка которых под случаи, предусмотренные ст. 6, ч.1, п.2 и п. 11 152-ФЗ, не подпадает, могут сами являться Операторами этих ПДн. В этом случае Оператор электронной площадки является лицом, выполняющим обработку этих ПДн по поручению этих Операторов ПДн в соответствии с 152-ФЗ ст.6, ч.3. Поручение в этом случае должно входить в состав соответствующего регламента (публичного договора присоединения) электронной площадки или двустороннего договора и соответствовать требованиям п. 10.8 (ч.3, ст.6, [1]).

10.16. В части обработки ПДн в целях [12], технологические и программные средства, используемые для ведения сайта, должны обеспечивать доступ пользователей к ознакомлению с информацией, размещенной на сайте, на основе распространенных веб-обозревателей. При этом не должна предусматриваться установка на компьютеры

пользователей технологических и программных средств, специально созданных для просмотра сайта.

10.17. Запрещается использование иностранных мессенджеров (Telegram, WhatsApp и т.п., см. https://rkn.gov.ru/docs/Perechen6_informacionnykh_sistem_05052023.pdf) для информирования граждан РФ ([17], ст.15, ч.1, п.2, п.5,), и (или) для передачи платежных документов и (или) предоставления информации, содержащей персональные данные граждан РФ, данных о переводах денежных средств в рамках применяемых форм безналичных расчетов, сведений, необходимых для осуществления платежей и (или) сведений о счетах (вкладах) граждан РФ в банках ([16], ст.10, ч.8).

11. ОСОБЕННОСТИ ОРГАНИЗАЦИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОСУЩЕСТВЛЯЕМОЙ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ

11.1. Обработка ПДн, содержащихся в ИСПДн либо извлеченных из такой системы (далее - персональные данные), считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение ПДн в отношении каждого из субъектов ПДн, осуществляются при непосредственном участии человека ([4], п.1).

11.2. Обработка ПДн не может быть признана осуществляемой с использованием средств автоматизации только на том основании, что персональные данные содержатся в информационной системе ПДн либо были извлечены из нее ([4], п.2).

11.3. Правила обработки ПДн, осуществляемой без использования средств автоматизации, установленные нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами организации, должны применяться с учетом требований [4].

11.4. ПДн при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях ПДн (далее - материальные носители), в специальных разделах или на полях форм (бланков) ([4], п.4). При фиксации ПДн на материальных носителях не допускается фиксация на одном материальном носителе ПДн, цели обработки которых заведомо не совместимы. Для обработки различных категорий ПДн, осуществляемой без использования средств автоматизации, для каждой категории ПДн должен использоваться отдельный материальный носитель ([4], п.5).

11.5. Лица, осуществляющие обработку ПДн без использования средств автоматизации (в том числе сотрудники организации-оператора или лица, осуществляющие такую обработку по договору с оператором), должны быть проинформированы о факте обработки ими ПДн, обработка которых осуществляется оператором без использования средств автоматизации, категориях обрабатываемых ПДн, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами организации (при их наличии) ([4], п.6). Данное информирование производится Оператором в отношении всех своих работников (в том числе работающих с Оператором по договору) путем доведения настоящего документа.

11.6. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них ПДн (далее - типовая форма), должны соблюдаться следующие условия ([4], п.7):

- типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки ПДн, осуществляемой без использования средств автоматизации, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес субъекта ПДн, источник получения ПДн, сроки

обработки ПДн, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки ПДн;

• типовая форма должна предусматривать поле, в котором субъект ПДн может поставить отметку о своем согласии на обработку ПДн, осуществляемую без использования средств автоматизации, - при необходимости получения письменного согласия на обработку ПДн;

• типовая форма должна быть составлена таким образом, чтобы каждый из субъектов ПДн, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов ПДн;

• типовая форма должна исключать объединение полей, предназначенных для внесения ПДн, цели обработки которых заведомо не совместимы.

11.7. При ведении журналов (реестров, книг), содержащих персональные данные, необходимые для однократного пропуска субъекта ПДн на территорию, на которой находится оператор, или в иных аналогичных целях, должны соблюдаться следующие условия ([4], п.8):

• необходимость ведения такого журнала (реестра, книги) должна быть предусмотрена актом оператора, содержащим сведения о цели обработки ПДн, осуществляемой без использования средств автоматизации, способы фиксации и состав информации, запрашиваемой у субъектов ПДн, перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги), сроки обработки ПДн, а также сведения о порядке пропуска субъекта ПДн на территорию, на которой находится оператор, без подтверждения подлинности ПДн, сообщенных субъектом ПДн;

• копирование содержащейся в таких журналах (реестрах, книгах) информации не допускается;

• персональные данные каждого субъекта ПДн могут заноситься в такой журнал (книгу, реестр) не более одного раза в каждом случае пропуска субъекта ПДн на территорию, на которой находится оператор.

11.8. При несовместимости целей обработки ПДн, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку ПДн отдельно от других зафиксированных на том же носителе ПДн, должны быть приняты меры по обеспечению раздельной обработки ПДн, в частности ([4], п.9):

• при необходимости использования или распространения определенных ПДн отдельно от находящихся на том же материальном носителе других ПДн осуществляется копирование ПДн, подлежащих распространению или использованию, способом, исключающим одновременное копирование ПДн, не подлежащих распространению и использованию, и используется (распространяется) копия ПДн;

• при необходимости уничтожения или блокирования части ПДн уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование ПДн, подлежащих уничтожению или блокированию. Уничтожение или обезличивание части ПДн, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих ПДн с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание) ([4], п.10).

11.9. Правила, предусмотренные двумя предыдущими пунктами настоящего Положения, применяются также в случае, если необходимо обеспечить раздельную обработку зафиксированных на одном материальном носителе ПДн и информации, не являющейся персональными данными ([4], п.11).

11.10. Уточнение ПДн при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными ([4], п.12).

11.11. Обработка ПДн, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории ПДн можно было определить места хранения ПДн (материальных носителей) и установить перечень лиц, осуществляющих обработку ПДн либо имеющих к ним доступ ([4], п.13).

11.12. Необходимо обеспечивать раздельное хранение ПДн (материальных носителей), обработка которых осуществляется в различных целях ([4], п.14).

11.13. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность ПДн 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 оператором ([4], п.15).

12. АКТУАЛИЗАЦИЯ, ИСПРАВЛЕНИЕ, УДАЛЕНИЕ И УНИЧТОЖЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОТВЕТЫ НА ЗАПРОСЫ СУБЪЕКТОВ НА ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ

12.1. Оператор обязан сообщить в порядке, предусмотренном статьей 14 [1], субъекту ПДн или его представителю информацию о наличии ПДн, относящихся к соответствующему субъекту ПДн, а также предоставить возможность ознакомления с этими ПДн при обращении субъекта ПДн или его представителя либо в течение десяти рабочих дней с даты получения запроса субъекта ПДн или его представителя. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления оператором в адрес субъекта ПДн мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации ([1], ст. 20, ч.1).

12.2. В случае отказа в предоставлении информации о наличии ПДн о соответствующем субъекте ПДн или ПДн субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта ПДн или его представителя оператор обязан дать в письменной форме мотивированный ответ, содержащий ссылку на положение ч. 8 ст. 14 [1] или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий десяти рабочих дней со дня обращения субъекта ПДн или его представителя либо с даты получения запроса субъекта ПДн или его представителя. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления оператором в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации. ([1], ст. 20, ч.2).

12.3. Оператор обязан предоставить безвозмездно субъекту ПДн или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту ПДн. В срок, не превышающий семи рабочих дней со дня предоставления субъектом ПДн или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, оператор обязан внести в них необходимые изменения. В срок, не превышающий семи рабочих дней со дня представления субъектом ПДн или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, оператор обязан уничтожить такие персональные данные. Оператор обязан уведомить субъекта ПДн или его представителя о

внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы ([1], ст. 20, ч.3).

12.4. Оператор обязан сообщить в уполномоченный орган по защите прав субъектов персональных данных по запросу этого органа необходимую информацию в течение десяти рабочих дней с даты получения такого запроса. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления оператором в адрес уполномоченного органа по защите прав субъектов персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации. ([1], ст. 20, ч.4).

12.5. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя либо по запросу субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных оператор обязан осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных оператор обязан осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц ([1], ст. 21, ч.1).

12.6. В случае подтверждения факта неточности персональных данных оператор на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязан уточнить персональные данные либо обеспечить их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных ([1], ст. 21, ч.2).

12.7. В случае выявления неправомерной обработки персональных данных, осуществляемой оператором или лицом, действующим по поручению оператора, оператор в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению оператора. В случае, если обеспечить правомерность обработки персональных данных невозможно, оператор в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган ([1], ст. 21, ч.3).

12.8. В случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных, оператор обязан с момента выявления такого инцидента оператором, уполномоченным органом по защите прав субъектов персональных

данных или иным заинтересованным лицом по защите прав субъектов персональных данных:

- в течение двадцати четырех часов о произошедшем инциденте, о предполагаемых причинах, повлекших нарушение прав субъектов персональных данных, и предполагаемом вреде, нанесенном правам субъектов персональных данных, о принятых мерах по устранению последствий соответствующего инцидента, а также предоставить сведения о лице, уполномоченном оператором на взаимодействие с уполномоченным органом по защите прав субъектов персональных данных, по вопросам, связанным с выявленным инцидентом;
- в течение семидесяти двух часов о результатах внутреннего расследования выявленного инцидента, а также предоставить сведения о лицах, действия которых стали причиной выявленного инцидента (при наличии).

12.9. В случае достижения цели обработки персональных данных оператор обязан прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных настоящим Федеральным законом или другими федеральными законами ([1], ст. 21, ч.4).

12.10. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных оператор обязан прекратить их обработку или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных настоящим Федеральным законом или другими федеральными законами ([1], ст. 21, ч.5).

12.11. В случае обращения субъекта ПДн к оператору с требованием о прекращении обработки ПДн оператор обязан в срок, не превышающий десяти рабочих дней с даты получения оператором соответствующего требования, прекратить их обработку или обеспечить прекращение такой обработки (если такая обработка осуществляется лицом, осуществляющим обработку ПДн), за исключением случаев, предусмотренных пунктами 2 - 11 части 1 статьи 6, частью 2 статьи 10 и частью 2 статьи 11 [1]. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления оператором в адрес субъекта GLy мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации ([1], ст. 21, ч.5.1).

12.12. В случае отсутствия возможности уничтожения ПДн в течение указанного срока оператор осуществляет блокирование таких ПДн или обеспечивает их блокирование (если обработка ПДн осуществляется другим лицом, действующим по поручению оператора) и обеспечивает уничтожение ПДн в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами ([1], ст. 21, ч.6).

12.13. Порядок обезличивания и уничтожения персональных данных.

12.13.1. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, в том числе установленных сроков хранения, если иное не предусмотрено федеральным законом.

12.13.2. Несанкционированное уничтожение персональных данных запрещено, в случае неумышленного уничтожения персональных данных Оператор восстанавливает персональные данные в полном объеме и за счет собственных средств.

12.13.3. Бумажные носители персональных данных, не требующие хранения (а также обязательной сдаче в архив Оператора) в рамках ведения делопроизводства, а также отсутствия таких требований в действующем законодательстве РФ, уничтожаются ответственным за них сотрудником в течение тридцати дней после прекращения трудовых или гражданско-правовых отношений с физическим лицом, Факт уничтожения оформляется соответствующим актом.

12.13.4. Уничтожение персональных данных, не подлежащих хранению в архиве Общества, осуществляется в течение тридцати рабочих дней с даты достижения цели обработки:

- данные на бумажных носителях уничтожаются с использованием уничтожителя бумаги (шредера);
- данные на машинных носителях стираются с многоразовых носителей средствами и способами, исключающими возможность восстановления информации, а с одноразовых машинных носителей – путем их механического разрушения.

13. МЕРЫ, НАПРАВЛЕННЫЕ НА ОБЕСПЕЧЕНИЕ ВЫПОЛНЕНИЯ ОПЕРАТОРОМ СВОИХ ОБЯЗАННОСТЕЙ, ПРЕДУСМОТРЕННЫХ ФЕДЕРАЛЬНЫМ ЗАКОНОМ ОТ 27.07.2006 N 152-ФЗ ("О ПЕРСОНАЛЬНЫХ ДАННЫХ"

13.1. Оператор принимает следующие меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных [1] и принятыми в соответствии с ним нормативными правовыми актами:

- назначает ответственного за организацию обработки ПДн ([1], ст.22.1);
- издает документы, определяющие политику оператора в отношении обработки персональных данных, локальные акты по вопросам обработки персональных данных, определяющие для каждой цели обработки персональных данных категории и перечень обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, способы, сроки их обработки и хранения, порядок уничтожения персональных данных при достижении целей их обработки или при наступлении иных законных оснований, а также локальные акты, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства РФ, устранение последствий таких нарушений. Такие документы и локальные акты не могут содержать положения, ограничивающие права субъектов персональных данных, а также возлагающие на оператора не предусмотренные законодательством Российской Федерации полномочия и обязанности ([1], ст.18.1, ч.1, п.2);
- применяет правовые, организационные и технические меры по обеспечению безопасности ПДн в соответствии со ст. 19 [1] ([1], ст.18.1, ч.1,п.3);
- осуществляет внутренний контроль и (или) аудит соответствия обработки ПДн [1] и принятым в соответствии с ним нормативным правовым актам, требованиям к защите

ПДн, политике оператора в отношении обработки ПДн, локальным актам оператора ([1], ст.18.1, ч.1,п.4);

- оценивает вред, который может быть причинен субъектам ПДн в случае нарушения настоящего Федерального закона, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных настоящим Федеральным законом([1], ст.18.1, ч.1,п.5);
- знакомит работников, непосредственно осуществляющих обработку ПДн, с положениями законодательства Российской Федерации о ПДн, в том числе требованиями к защите ПДн, документами, определяющими политику оператора в отношении обработки ПДн, локальными актами по вопросам обработки ПДн, и (или) обучение указанных работников ([1], ст.18.1, ч.1,п.6).

13.2. Оператор публикует настоящую Политику в отношении обработки ПДн, сведения о реализуемых требованиях к защите ПДн. Оператор публикует в информационно-телекоммуникационной сети Интернет, в том числе на страницах принадлежащего оператору сайта, с использованием которых осуществляется сбор персональных данных, настоящий документ, определяющий его политику в отношении обработки ПДн, и сведения о реализуемых требованиях к защите ПДн, а также обеспечивает возможность доступа к указанному документу с использованием средств информационно-телекоммуникационной сети Интернет ([1], ст.18.1, ч.2).

13.3. Оператор представляет документы и локальные акты, указанные в настоящем разделе подтверждающие принятие мер, указанных в настоящем разделе по запросу уполномоченного органа по защите прав субъектов ПДн ([1], ст.18.1, ч.3).

14. МЕРЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ

14.1. Оператор при обработке ПДн принимает необходимые правовые, организационные и технические меры для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн ([1], ст.19, ч.1).

14.2. Оператор реализует следующие меры по обеспечению защиты ПДн ([1], ст.19, ч.1):

- в соответствии с [8] определяет модель угроз безопасности ПДн при их обработке в ИСПДн ([1], ст.19, ч.2, п.1);
- применяет организационные и технические меры по обеспечению безопасности ПДн при их обработке в информационных системах ПДн, необходимые для выполнения требований к защите ПДн, исполнение которых обеспечивает установленные [3] уровни защищенности ПДн ([1], ст.19, ч.2, п.2);
- применяет прошедшие в установленном порядке процедуру оценки соответствия средств защиты информации ([1], ст.19, ч.2, п.3);;
- оценивает эффективность принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию ИСПДн ([1], ст.19, ч.2, п.4);
- проводит учет машинных носителей ([1], ст.19, ч.2, п.1) в случаях, установленных [7];
- обнаруживает факты несанкционированного доступа к персональным данным и принимает меры, в том числе меры по обнаружению, предупреждению и ликвидации последствий компьютерных атак на ИСПДн и по реагированию на компьютерные инциденты в них ([1], ст.19, ч.2, п.6);;
- обеспечивает восстановление ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним ([1], ст.19, ч.2, п.7);

- устанавливает правила доступа к персональным данным, обрабатываемым в ИСПДн, а также обеспечивает регистрацию и учет всех действий, совершаемых с персональными данными в ИСПДн ([1], ст.19, ч.2, п.8);
- ведет контроль за принимаемыми мерами по обеспечению безопасности ПДн и уровня защищенности ИСПДн ([1], ст.19, ч.2, п.9);.

14.3. Оператор реализует требования [3] и [9], определяющие:

- уровни защищенности ПДн при их обработке в ИСПДн в зависимости от угроз безопасности этих данных;
- требования к защите ПДн при их обработке в ИСПДн, исполнение которых обеспечивает установленные уровни защищенности ПДн;

В соответствии с [1], ст.19, ч.3 указанные требования уже учитывают:

- возможный вред субъекту ПДн, чем достигается выполнение [1], ст.18.1, ч.1, п.5 по вопросу соотношения указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных [1];;
- объем и содержание обрабатываемых ПДн;
- вид деятельности, при осуществлении которого обрабатываются персональные данные;
- актуальные угрозы безопасности ПДн.

14.4. Состав и содержание указанных в п.14.3 требований к защите ПДн для каждого из уровней защищенности, организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн устанавливаются [6], [7], [10].

14.5. Контроль и надзор за выполнением организационных и технических мер по обеспечению безопасности ПДн, установленных в соответствии с настоящей статьей, при обработке ПДн в государственных ИСПДн осуществляются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий и без права ознакомления с персональными данными, обрабатываемыми в ИСПДн.

14.6. Федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, и федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации, решением Правительства Российской Федерации с учетом значимости и содержания обрабатываемых ПДн могут быть наделены полномочиями по контролю за выполнением организационных и технических мер по обеспечению безопасности ПДн, установленных в соответствии с настоящей статьей, при их обработке в ИСПДн, эксплуатируемых при осуществлении определенных видов деятельности и не являющихся государственными ИСПДн, без права ознакомления с ПДн, обрабатываемыми в ИСПДн.

14.7. Оператор обязан в порядке, определенном федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, обеспечивать взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, включая информирование его о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных ([1], ст.19, ч.12). Порядок передачи этой информации устанавливается совместно федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и уполномоченным органом по защите прав субъектов персональных данных ([1], ст.19, ч.13).

15. ВНУТРЕННИЙ КОНТРОЛЬ

Оператор обязан осуществлять внутренний контроль и (или) аудит соответствия обработки персональных данных [1] и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора ([1], ст.18.1. ч.1, п.4).

Внутренний контроль, в том числе требований к защите персональных данных, осуществляет лицо, ответственное за организацию обработки персональных данных, в частности, обязано ([1], ст.22.1. ч.4).

Указанный контроль проводится не реже 1 раза в 3 года в сроки, определяемые оператором ([3], п.17).

Внутренний контроль организуется и проводится оператором самостоятельно и (или) с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации ([3], п.17).

До начала внутреннего контроля разрабатывается календарный план его проведения.

В ходе внутреннего контроля производится:

- контроль соблюдения оператором и его работниками законодательства РФ о персональных данных, в том числе требований к защите персональных данных (установлен [1], п.4, ч.1, ст.18.1, п.1, ч.4, ст.22.1, п.4, ч.2, ст.19);
- контроль выполнения Постановления Правительства РФ от 1 ноября 2012 г. N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" (установлен п. 17 этого Постановления);
- оценка эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных (установлена Приказом Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. N 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности, п.6);
- разработка организационных и технических рекомендаций (мер), а также проектов внутренних нормативных документов (или предложений по их доработке) по устранению выявленных несоответствий законодательным и нормативным требованиям.

Результаты внутреннего контроля отражаются в отчете.

16. ПЕРЕЧЕНЬ ССЫЛОЧНЫХ ДОКУМЕНТОВ

1. 152-ФЗ 2006 г. «О персональных данных».
2. "Трудовой кодекс Российской Федерации" от 30.12.2001 N 197-ФЗ.
3. Постановление Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных".
4. Постановление Правительства РФ от 15.09.2008 N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации".
5. Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 24 февраля 2021 г. N 18 "Об утверждении требований к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения".
6. Приказ Федеральной службы по техническому и экспортному контролю от 11 апреля 2025 г. N 117 " Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах

государственных органов, государственных унитарных предприятий, государственных учреждений".

7. Приказ Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. N 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных".

8. Методический документ "Методика оценки угроз безопасности информации" (утв. Федеральной службой по техническому и экспортному контролю 5 февраля 2021 г.).

9. Постановление Правительства РФ от 08.06.2018 N 656 "О требованиях к операторам электронных площадок, операторам специализированных электронных площадок, электронным площадкам, специализированным электронным площадкам и функционированию электронных площадок, специализированных электронных площадок, подтверждении соответствия таким требованиям, об утрате юридическим лицом статуса оператора электронной площадки, оператора специализированной электронной площадки" (вместе с "Правилами подтверждения соответствия электронной площадки, специализированной электронной площадки, оператора электронной площадки, оператора специализированной электронной площадки единым требованиям к операторам электронных площадок, операторам специализированных электронных площадок, электронным площадкам, специализированным электронным площадкам и функционированию электронных площадок, специализированных электронных площадок и дополнительным требованиям к операторам электронных площадок, операторам специализированных электронных площадок и функционированию электронных площадок, специализированных электронных площадок", "Правилами утраты юридическим лицом статуса оператора электронной площадки, оператора специализированной электронной площадки для целей Федерального закона "О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд").

10. Приказ ФСБ России от 10.07.2014 N 378 "Об утверждении Состава 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 требований к защите персональных данных для каждого из уровней защищенности".

11. 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".

12. Постановление Правительства РФ от 17.03.2008 N 179 "Об утверждении Положения о пользовании сайтами в сети Интернет, на которых осуществляется проведение открытых аукционов в электронной форме, и требованиях к технологическим, программным, лингвистическим, правовым и организационным средствам обеспечения пользования указанными сайтами, а также к системам, обеспечивающим проведение открытых аукционов в электронной форме".

13. Федеральный закон от 06.04.2011 N 63-ФЗ "Об электронной подписи".

14. Рекомендации Роскомнадзора РФ по составлению документа, определяющего политику Оператора в отношении обработки ПДн (см. https://rkn.gov.ru/personal-data/p908/), редакция от 01.08.2017.

15. Национальный стандарт РФ ГОСТ Р 59407-2021 "Информационные технологии. Методы и средства обеспечения безопасности. Базовая архитектура защиты персональных данных".

16. Федеральный закон от 27 июля 2006 г. № 149-ФЗ "Об информации,

информационных технологиях и о защите информации".

17. Федеральный закон от 1 апреля 2025 г. N 41-ФЗ "О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации".

Приложение 1 к Политике в отношении обработки
персональных данных в АО «Сбербанк-АСТ»

Порядок
реагирования на обращения и запросы по вопросам обработки персональных данных в АО «Сбербанк-АСТ»

1. ОБЩИЕ ТРЕБОВАНИЯ К ЗАПРОСАМ

Оператор принимает запросы только от самого субъекта ПДн или его законного представителя (по предъявлении документа, подтверждающего его полномочия).

В случаях п.1.1 – 1.3 запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Оператором, подпись субъекта персональных данных или его представителя ([1], ст.14, ч.3).

Возможные виды запросов субъектов ПДн, требования к их содержанию и срокам исполнения:

1.1. **Получение сведений об обработке своих ПДн** (ч. 7, ст. 14, [1]), включая возможность ознакомления с этими ПДн (ч. 1, ст. 20, [1]). Срок ответа оператора – 10 рабочих дней, возможное продление этого срока – до 5 рабочих дней.

Перечень запрашиваемой информации должен соответствовать ч. 7, ст. 14, [1], а в случае запроса по п. 10, ч. 7, ст. 14, [1]: «иные сведения, предусмотренные настоящим Федеральным законом или другими федеральными законами» необходима ссылка на соответствующие основания - конкретные пункты этих законов.

1.2. **Требование к Оператору уточнения ПДн, их блокирования или уничтожения** в случае, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки (ч. 1, ст. 14, [1]). Срок ответа оператора – 10 рабочих дней, возможное продление этого срока – до 5 рабочих дней. Срок внесения оператором изменений или уничтожения ПДн – 7 рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки.

Запрос должен содержать сведения, подтверждающие, что персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки.

1.3. **Требование к Оператору прекращения обработки ПДн** (ч. 5.1, ст. 21, [1]), включая требование к Оператору прекращения обработки ПДн, производимой с целью «продвижения товаров, работ, услуг» (ч. 2, ст. 15, [1]). Срок прекращения оператором обработки ПДн – немедленно. Срок ответа оператора – 10 рабочих дней, возможное продление этого срока – до 5 рабочих дней.

1.4. **Требование к Оператору о прекращении распространения ПДн**, разрешенных субъектом персональных данных для распространения. Запрос должен включать в себя фамилию, имя, отчество (при наличии), контактную информацию (номер телефона, адрес электронной почты или почтовый адрес) субъекта ПДн, а также перечень персональных данных, обработка которых подлежит прекращению (ч. 12, ст. 10.1, [1]). Срок прекращения оператором обработки ПДн – немедленно (ч. 13, ст. 10.1, [1]).

2. ПОРЯДОК НАПРАВЛЕНИЯ ЗАПРОСА ОПЕРАТОРУ

Запрос субъекта ПДн должен быть направлен на официальный почтовый адрес или адрес электронной почты Оператора, указанный на его сайте https://www.sberbank-ast.ru/ , либо доставлен субъектом ПДн (или его законным представителем) лично.

В случае личной доставки субъект ПДн или его представитель должен иметь при себе документ, удостоверяющий его личность. Работник Оператора при приеме запроса должен сверить указанные в запросе данные заявителя с его документом, удостоверяющим личность, и зарегистрировать запрос. По требованию субъекта ПДн или его представителя сообщить регистрационный номер запроса.

Запрос в форме электронного документа должен быть подписан квалифицированной электронной подписью в соответствии с законодательством Российской Федерации ([1], ст.14, ч.3). Получить подтверждение получения Оператором запроса отправитель может с использованием функционала подтверждения электронной почты (в электронном письме включить галочку подтверждения получения), либо по телефону от службы техподдержки Оператора.

Оператор может отказать в приеме запросов, не соответствующих вышеуказанным требованиям. О причинах отказа он информирует отправителя запроса.

3. ПОРЯДОК ПРИЕМА ЗАПРОСОВ ОПЕРАТОРОМ

Прием и регистрация запросов субъектов персональных данных производится подразделением делопроизводства Оператора в соответствии с общими правилами обработки входящей корреспонденции. Далее запросы в установленном порядке направляются на исполнение работнику Оператора, ответственному за организацию обработки персональных данных и регистрируются им в журнале регистрации запросов и обращений субъектов персональных данных в день их поступления. Форма журнала регистрации запросов и обращений субъектов приведена в Приложении 1 к настоящему Регламенту.

Срок хранения запросов и ответов на них в соответствии с [11] составляет 5 лет.

4. ПОРЯДОК ОБРАБОТКИ ЗАПРОСОВ ОПЕРАТОРОМ

Обработка поступивших запросов производится работником Оператора, ответственным за организацию обработки персональных данных, в соответствии с требованиями и сроками, установленными [1], глава 3, ст.20 и представленными в [3], п.3.3, раздел 12. При необходимости он привлекает к этому других работников Оператора, а также в рабочем порядке может дозапрашивать у субъекта персональных данных (или его представителя) недостающую информацию.

При обработке запроса им производится:

- анализ соответствия запроса требованиям [1], глава 3, представленными в [3], п.3.3, другим требованиям [1] и подзаконных актов. При несоответствии готовится мотивированный отказ в его удовлетворении. Несущественные для данного запроса несоответствия (не влияющие на суть ответа) по решению Оператора могут быть проигнорированы;
- оценка времени, оставшегося для отправки ответа в установленные сроки;
- проверка изложенных в запросе фактов и событий, если они влияют на суть ответа;
- оценка необходимости каких-либо действий с ПДн заявителя, а также наличия требуемых для этого сил и средств. При подтверждении необходимости данные действия предпринимаются силами Владельца и Администратора соответствующих ИСПДн Оператора с использованием требуемых для этого административных прав и функционала ИСПДн. При обработке ПДн заявителя внешним обработчиком по договору с Оператором, должностное лицо Оператора, ответственное за взаимодействие с этим обработчиком, инициирует выполнение обработчиком требуемых действий и получает от него требуемые

подтверждения их выполнения. Предпринятые действия и их результат отражаются в ответе на запрос;

- подготовка ответа на запрос. Проект ответа согласовывается со всеми должностными лицами Оператора, имеющими отношение к сути запроса, после чего направляется в подразделение делопроизводства для его подписания уполномоченным должностным лицом Оператора, регистрации в системе делопроизводства и отправки заявителю.

5. ПОРЯДОК НАПРАВЛЕНИЯ ОТВЕТОВ

Подписанный и зарегистрированный ответ на запрос подразделение делопроизводства Оператора отправляет тем же способом, которым был получен запрос, если в запросе не был указан иной способ. Иначе и при наличии возможности – способом, указанным в запросе.

6. ПЕРЕЧЕНЬ ССЫЛОЧНЫХ ДОКУМЕНТОВ

1. 152-ФЗ 2006 г. «О персональных данных».
2. Рекомендации Роскомнадзора РФ по составлению документа, определяющего политику Оператора в отношении обработки ПДн (см. https://rkn.gov.ru/personal-data/p908/), редакция от 01.08.2017.
3. Политика в отношении обработки персональных данных в АО «Сбербанк-АСТ».

Приложение 1
К Порядку реагирования на обращения и запросы по вопросам обработки персональных данных
в **АО «Сбербанк-АСТ»**

ЖУРНАЛ
учета запросов (обращений) субъектов персональных данных
(форма для ведения журнала в бумажном виде)

№ п/п	Дата и рег. номер запроса (обращения)	Сведения о запрашивающем лице (Ф.И.О., паспортные данные)	Краткое содержание обращения	Отметка о предоставлении (отказе в предоставлении) информации	Дата и рег. номер ответа на запрос	Подпись запрашивающего лица о получении ответа (отметка об отправке письма)	Подпись ответственного лица
1.							
2.							
3.							

Примечание: допускается ведение учета запросов (обращений) субъектов персональных данных в электронном виде. При использовании системы простых файлов каждой записи журнала должна соответствовать папка (каталог) в файловой системе электронного носителя информации, содержащая информацию в объеме, не менее приведенной для журнала в бумажном виде.

Приложение 2 к Политике в отношении обработки персональных данных в АО «Сбербанк-АСТ»

Форма запроса о предоставлении третьим лицом, которому поручена обработка ПДн, документов и иной информации, подтверждающих принятие мер и соблюдение в целях исполнения поручения, установленных в соответствии с ч. 3 ст. 6 Закона №152-ФЗ

Уважаемый_____!

В соответствии с договором поручения обработки персональных данных №____ от_____ (или в целях заключения такого договора, если договор еще не заключен) и в соответствии с 152-ФЗ 2006 г. «О персональных данных», ст. 6, ч.3, прошу представить документы и иную информацию, подтверждающие принятие мер и соблюдение в целях исполнения поручения оператора требований, установленных в соответствии с вышеуказанной статьей, обязанность обеспечивать безопасность персональных данных при их обработке.

Примечание: запрос направляется официальным письмом за подписью уполномоченного на ведение такой переписки должностного лица в соответствии с установленным порядком делопроизводства.

Приложение 3 к Политике в отношении обработки
персональных данных в АО «Сбербанк-АСТ»

Порядок оценки соблюдения третьим лицом, которому поручена обработка ПДн, конфиденциальности и обеспечения безопасности ПДн при их обработке

Оценки соблюдения третьим лицом, которому поручена обработка ПДн, конфиденциальности и обеспечения безопасности ПДн при их обработке, производится Оператором по факту наличия Аттестата соответствия информационной системы персональных данных третьего лица требованиям по защите информации, установленным ФСТЭК РФ для требуемого в соответствии с Постановлением Правительства № 1119 2012 г. уровня защиты персональных данных.

Приложение 4 к Политике в отношении обработки
персональных данных в АО «Сбербанк-АСТ»

Типовая форма поручения обработки ПДн, в том числе содержащая сроки уведомления третьим лицом, которому поручена обработка ПДн, об инцидентах, повлекших неправомерную или случайную передачу (предоставление, распространение, доступ) ПДн

В соответствии с настоящим договором (либо на основании акта №___ от____ государственного или муниципального органа) или Оператор поручает <указать вторую сторону договора> обработку персональных данных с согласия субъекта персональных данных (или иное, если предусмотрено федеральным законом).

Лицо, осуществляющее обработку персональных данных по поручению Оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные 152-ФЗ 2006 г, соблюдать конфиденциальность персональных данных, принимать необходимые меры, направленные на обеспечение выполнения обязанностей, предусмотренных 152-ФЗ 2006 г., требований, предусмотренных частью 5 статьи 18, статьей 18.1 и статьей 19 152-ФЗ 2006 г.

Перечень обрабатываемых персональных данных:

_____

Перечень действий (операций) с персональными данными:

_____

Цели обработки:

_____

По запросу оператора персональных данных в течение срока действия поручения оператора, в том числе до обработки персональных данных, Исполнитель обязан предоставлять документы и иную информацию, подтверждающие принятие мер и соблюдение в целях исполнения поручения оператора требований, установленных в соответствии с 152-ФЗ 2006 г.,ст. 6, ч.3, в том числе требование об уведомлении оператора о случаях, предусмотренных частью 3.1 статьи 21 152-ФЗ 2005 г.

Сроки уведомления Исполнителем, об инцидентах, повлекших неправомерную или случайную передачу (предоставление, распространение, доступ) ПДн – незамедлительно (но с учетом ограничений Трудового Кодекса РФ).

Уведомление Исполнителем Оператора производится по форме, установленной Роскомнадзором https://pd.rkn.gov.ru/incidents/form/

Примечание: Поручение обработки ПДн может быть как самостоятельным договором, так и входить в состав других договоров в качестве отдельного раздела.

Приложение 5 к Политике в отношении обработки персональных данных в АО «Сбербанк-АСТ»

Типовая форма уведомления оператора об инцидентах, повлекших неправомерную или случайную передачу (предоставление, распространение, доступ) ПДн.

Уведомление Исполнителем Оператора производится по форме, установленной Роскомнадзором https://pd.rkn.gov.ru/incidents/form/