Утверждено приказом
ООО «ЛОУДЕР ЭСПИИКС»
№ ____ от «09» января 2023 г.

ПОЛОЖЕНИЕ
ОБ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

2023 год

Москва

СОДЕРЖАНИЕ

1. СОКРАЩЕНИЯ, ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

1.1. Термины и определения

В настоящем документе использованы следующие термины и определения:

1.1.1. **Безопасность персональных данных** – состояние защищенности персональных данных от неправомерных действий, характеризуемое способностью пользователей, технических средств и информационных систем обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке, независимо от формы их представления.

1.1.2. **Биометрические персональные данные** – сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность.

1.1.3. **Внутренняя типовая форма** – документ, состав данных и порядок обработки которого не установлен законодательством РФ, и использующийся во внутренних бизнес-процессах Компании.

1.1.4. **Доступность персональных данных** – возможность беспрепятственного получения санкционированного доступа к персональным данным лицами, имеющими право на такой доступ.

1.1.5. **Защита информации** – деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

1.1.6. **Информационная система персональных данных** – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

1.1.7. **Инцидент безопасности персональных данных** – любое непредвиденное или нежелательное событие, которое может нарушить безопасность персональных данных, что может повлечь за собой нарушение деятельности Компании.

1.1.8. **Конфиденциальность персональных данных** – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не раскрывать третьим лицам и не допускать их распространения при отсутствии согласия субъекта персональных данных или иного законного основания.

1.1.9. **Несанкционированный доступ (несанкционированные действия)** – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

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

1.1.11. **Персональные данные** – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

1.1.12. **Пользователь персональных данных** – лицо, участвующее в процессе обработки персональных данных или использующее результаты такой обработки.

1.1.13. **Процесс обработки** персональных данных – бизнес-процесс Компании, в рамках которого осуществляется обработка персональных данных.

1.1.14. **Средство вычислительной техники** – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

1.1.15. **Средство защиты информации** – техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

1.1.16. **Угрозы безопасности персональных данных** – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

1.1.17. **Уничтожение персональных данных** – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

1.1.18. **Целостность персональных данных** – способность средства вычислительной техники или информационной системы обеспечивать неизменность персональных данных в условиях случайного и/или преднамеренного их искажения (разрушения).

1.2. Используемые сокращения

В настоящем документе использованы сокращения, приведенные в Таблице 1:

Таблица 1. Сокращения

Сокращение	Описание
ИСПДн	Информационная система персональных данных
ПДн	Персональные данные
СЗПДн	Система защиты персональных данных

2. НАЗНАЧЕНИЕ И ОБЛАСТЬ ДЕЙСТВИЯ ДОКУМЕНТА

2.1. В настоящем Положении об обработке персональных данных (далее – "Положение") установлены требования по организации и непосредственному функционированию процессов обработки ПДн в Обществе с ограниченной ответственностью «ЛОУДЕР ЭСПИИКС» (далее – "Компания") в соответствии с требованиями нормативных правовых актов Российской Федерации в области обработки и обеспечения безопасности ПДн.

2.2. Требования настоящего Положения распространяются на структурные подразделения Компании и отдельных должностных лиц, принимающих участие в процессах обработки ПДн.

2.3. Требования настоящего Положения распространяются на все процессы обработки ПДн, независимо от формы их представления.

3. ОБЩИЕ ПОЛОЖЕНИЯ

3.1. Настоящее Положение определяет:

- принципы обработки ПДн;
- виды обрабатываемых ПДн;
- жизненный цикл ИСПДн;
- состав системы защиты персональных данных;
- правила обработки ПДн;
- требования по обучению персонала в области обработки ПДн;

– требования по организации доступа к ПДн;

– требования к взаимодействию с субъектами ПДн и органами власти;

– требования к составу и содержанию документов Компании, регламентирующих обработку и защиту ПДн.

3.2. Настоящее Положение разработано в соответствии со следующими нормативными правовыми документами:

– Конституция Российской Федерации.

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

– Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

– Постановление Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

– Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

– Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (утвержден Приказом ФСТЭК России от 18.02 2013 № 21).

3.3. При работе с ПДн, во всех случаях, не урегулированных внутренними нормативными документами Компании, необходимо руководствоваться действующим законодательством РФ.

3.4. Настоящее Положение должно быть доведено до всех работников Компании под подпись. Подпись работника на листе ознакомления означает его согласие со всеми требованиями, указанными в настоящем Положении.

4. ПРИНЦИПЫ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. В соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» обработка ПДн в Компании должна осуществляться в соответствии со следующими принципами:

4.1.1. Обработка ПДн должна осуществляться на законной и справедливой основе.

4.1.2. Обработка ПДн должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка ПДн, несовместимая с целями их сбора.

4.1.3. Не допускается объединение баз данных, содержащих ПДн, обработка которых осуществляется в целях, несовместимых между собой.

4.1.4. Обработке подлежат только ПДн, которые отвечают целям их обработки.

4.1.5. Содержание и объем обрабатываемых ПДн должны соответствовать заявленным целям обработки. Обрабатываемые ПДн не должны быть избыточными по отношению к заявленным целям их обработки.

4.1.6. При обработке ПДн должны быть обеспечены их точность, достаточность, а в необходимых случаях и актуальность по отношению к целям обработки ПДн. Необходимо принимать меры по удалению или уточнению неполных или неточных данных.

4.1.7. 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 ПДн подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

4.1.8. Не допускается использовать ПДн в целях причинения имущественного и (или) морального вреда субъектам ПДн, затруднения реализации их прав и свобод.

4.1.9. Все работники должны быть ознакомлены под подпись с документами Компании, устанавливающими порядок обработки их ПДн, а также их правами и обязанностями в этой области, в соответствии с действующими нормативными документами.

4.2. В Компании должен проводиться регулярный анализ соответствия процессов обработки ПДн указанным выше принципам. Данный анализ проводится в следующих случаях:

– создание новых или внесение изменений в существующие процессы обработки ПДн;

– создание новых или внесение изменений в существующие ИСПДн;

– изменение нормативной базы, затрагивающей принципы и (или) процессы обработки ПДн в Компании;

– проведение внутренних контрольных мероприятий на предмет оценки соответствия процессов обработки ПДн заявленным принципам.

Трансграничная передача ПДн Компанией не осуществляется.

5. ОБРАБАТЫВАЕМЫЕ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

5.1. Отнесение сведений, обрабатываемых в Компании, к категории ПДн представляет собой процесс обоснованного установления (документального оформления и утверждения руководством Компании) критериев их выделения из всей совокупности обрабатываемых сведений.

5.2. В качестве таких критериев в отношении ПДн в Компании разрабатывается и утверждается документ «Перечень персональных данных, обрабатываемых в ООО «ЛОУДЕР ЭСПИИКС» (далее – Перечень ПДн). В Перечне ПДн закрепляются категории субъектов ПДн, группы и детальный состав ПДн, цели и правовые основания обработки для каждой из групп и категорий субъектов ПДн, а также сроки обработки и хранения ПДн.

5.3. В Компании осуществляется обработка ПДн, касающаяся состояния здоровья физических лиц, в рамках осуществления деятельности, направленной на выявление, оценку и предупреждение нежелательных реакций или любых других возможных проблем, связанных с лекарственными препаратами.

5.4. В Компании не допускается обработка ПДн, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений и интимной жизни.

6. ИНФОРМАЦИОННЫЕ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. Комплексы баз данных, средства вычислительной техники, технических средств обработки объединяются в информационные системы персональных данных. При этом в одну ИСПДн может входить любое количество компонентов.

6.2. Для каждой ИСПДн Компании в обязательном порядке должны быть разработаны следующие документы:

– Модель угроз безопасности ПДн при их обработке в ИСПДн.

– Модель нарушителя в ИСПДн (может включаться в Модель угроз безопасности ПДн в ИСПДн).

– Акт определения уровня защищенности ПДн при их обработке в ИСПДн.

6.3. Жизненный цикл ИСПДн Компании состоит из следующих стадий:

– проектирование;

– создание;

– эксплуатация;

– модернизация;

– вывод из эксплуатации.

6.4. Работы по данным стадиям проводятся в соответствии с Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», а также Приказом ФСТЭК России от 18.02.2013 № 21 «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

6.5. Порядок проведения необходимых мероприятий в рамках жизненного цикла ИСПДн описан в документе «Положение по обеспечению безопасности персональных данных».

7. СИСТЕМА ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1. С целью выполнения требований законодательства РФ в области ПДн, Компания считает важнейшей задачей обеспечение конфиденциальности, целостности и доступности ПДн при их обработке.

7.2. Для решения данной задачи в Компании введена, функционирует и проходит периодический пересмотр (контроль) Система защиты персональных данных, которая состоит из следующих компонентов:

– организационная структура (участники обработки и ответственные лица);

– организационно-распорядительная документация;

– средства обработки ПДн;

– меры и средства обеспечения безопасности ПДн.

7.3. СЗПДн Компании основана на следующих принципах:

– вовлеченность руководства – деятельность по обеспечению безопасности ПДн инициирована и контролируется руководством Компании;

– соответствие мер и средств защиты актуальным угрозам безопасности ПДн;

– соответствие мер и средств защиты требованиям нормативных документов РФ в области обработки и обеспечения безопасности ПДн;

– комплексность – с целью обеспечения безопасности ПДн в Компании используется совокупность организационных и технических мер;

– патентная чистота – средства защиты информации, входящие в состав СЗПДн Компании, отвечают требованиям по обеспечению патентной чистоты согласно действующим нормативным документам РФ. Используемое общесистемное, специальное и прикладное программное обеспечение имеет соответствующие лицензии производителей;

– удобство персонала – при построении и модернизации СЗПДн в Компании учитываются и, по возможности, сводятся к минимуму возможные затруднения персонала в работе со средствами защиты и при выполнении основных процедур обеспечения безопасности ПДн;

– законность организационных и технических мер по обеспечению безопасности ПДн;

– непрерывность повышения уровня знаний работников Компании в сфере обеспечения безопасности ПДн;

– стремление к постоянному совершенствованию СЗПДн.

7.4. В соответствии с принципами обработки ПДн в Компании определены правила обработки ПДн, а также методы и способы обеспечения безопасности ПДн.

7.5. Конкретные методы и способы обеспечения безопасности ПДн, а также порядок их реализации описаны в документах:

– Положение по обеспечению безопасности персональных данных.

– Инструкция работника по правилам обработки и обеспечения безопасности персональных данных.

8. ОРГАНИЗАЦИОННАЯ СТРУКТУРА КОМПАНИИ В СФЕРЕ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

8.1. С целью организации и контроля обработки и обеспечения безопасности ПДн, в Компании вводятся следующие роли, которые составляют основу организационной структуры Компании в сфере обработки ПДн:

1) Ответственный за организацию обработки ПДн;

2) Ответственный за обеспечение безопасности ПДн;

3) Руководитель структурного подразделения;

4) Пользователь ПДн.

8.2. Функции указанных ролей приведены в Таблице 2. При распределении ответственности за мероприятия (функции) в таблице используются следующие сокращения степени участия в выполнении функций:

– «О» – организация и контроль;

– «И» – исполнение;

– «С» – согласование;

– «сИ» – соисполнение.

Таблица 2. Распределение ответственности за выполнение мероприятий в области обработки и защиты ПДн

№ п/п	Наименование мероприятия	Ответственный за организацию обработки ПДн	Ответственный за обеспечение безопасности ПДн	Руководитель структурного подразделения	Пользователь ПДн	Комиссия
1	***Взаимодействие с работниками Компании***					
1.1	Доведение до работников Компании положений законодательства РФ и требований внутренней документации в области ПДн	О, И	сИ	сИ	–	–
1.2	Предоставление консультаций и рекомендаций Пользователям ПДн по вопросам обработки и обеспечения безопасности ПДн	–	О, И	сИ	–	–
1.3	Инструктаж работников по правилам обработки ПДн	–	О, И	сИ	–	–
2	***Взаимодействие с субъектами ПДн и органами власти***					
2.1	Взаимодействие с субъектами ПДн или их представителями (обработка запросов, обращений, уведомление субъектов, сбор согласий на обработку ПДн)	О	–	И	–	–
2.2	Взаимодействие с регулирующими органами (Роскомнадзор, ФСТЭК России, ФСБ России) и иными органами власти	О, И	сИ	–	–	–
3	***Создание ИСПДн***					
3.1	Определение ключевых сведений об ИСПДн	–	–	сИ	–	О, И
3.2	Правовая оценка возможности создания (модернизации) ИСПДн	–	–	–	–	О, И

№ п/п	Наименование мероприятия	Ответственный за организацию обработки ПДн	Ответственный за обеспечение безопасности ПДн	Руководитель структурного подразделения	Пользователь ПДн	Комиссия
4	***Мониторинг и планирование***					
4.1	Мониторинг изменений законодательства РФ в области ПДн	О, И	сИ	–	–	–
4.2	Мониторинг СЗПДн	–	–	сИ	–	О, И
4.3	Планирование мероприятий по обеспечению безопасности СЗПДн (в т. ч. пересмотр СЗПДн)	–	–	–	–	О, И
5	***Эксплуатация СЗПДн***					
5.1	Поддержание работоспособности компонентов СЗПДн	–	О, И	сИ	–	–
5.2	Управление доступом работников к ПДн	–	С, И	О	–	–
5.3	Управление доступом третьих сторон к ПДн	О, И	–	–	–	–
5.4	Поручение обработки ПДн	О, И	–	–	–	–
5.5	Учет и уничтожение машинных носителей ПДн	–	О, И	–	–	–
5.6	Хранение бумажных и машинных носителей ПДн	–	–	О	И	–
5.7	Уничтожение бумажных носителей ПДн в рабочем порядке	–	–	О	И	–
5.8	Централизованное уничтожение бумажных носителей ПДн	–	–	–	–	О
5.9	Контроль доступа на территорию Компании	–	О	–	–	–

№ п/п	Наименование мероприятия	Ответственный за организацию обработки ПДн	Ответственный за обеспечение безопасности ПДн	Руководитель структурного подразделения	Пользователь ПДн	Комиссия
5.10	Контроль доступа в помещения с оборудованием ИСПДн	–	О	–	–	–
5.11	Контроль доступа к техническим средствам ИСПДн	–	О, И	сИ	–	–
5.12	Контроль перемещений физических компонентов ИСПДн	–	О, И	–	–	–
5.13	Резервирование ПДн	–	О, И	–	–	–
5.14	Расследование инцидентов безопасности ПДн	–	И	сИ	–	О
5.15	Внутренние контрольные мероприятия и корректирующие действия по их результатам	–	–	–	–	О

9. ПРАВИЛА ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

9.1. Политика в отношении обработки персональных данных

9.1.1. В целях обеспечения неограниченного доступа к документу, определяющему политику Компании в отношении обработки ПДн и к сведениям о реализуемых требованиях к защите ПДн, в Компании разработан документ «Политика обработки и обеспечения безопасности персональных данных» (далее – Открытая политика).

9.1.2. Открытая политика разрабатывается на основе сведений, указанных в данном Положении, и в частности содержит:

– принципы обработки ПДн;

– категории субъектов ПДн;

– основные правила обработки ПДн;

– права субъектов ПДн;

– реализуемые требования по обеспечению безопасности ПДн.

9.2. Сбор персональных данных

9.2.1. Компания получает ПДн из следующих источников:

– непосредственно от субъекта ПДн;

– от третьей стороны, в целях исполнения договорных обязательств или исполнения требований нормативных документов РФ;

– от другого субъекта ПДн, в целях реализации его законных прав.

9.2.2. Если предоставление ПДн является обязательным в соответствии с федеральным законом и субъект ПДн отказывается предоставить его ПДн, необходимо разъяснить субъекту ПДн юридические последствия такого отказа.

9.2.3. При сборе ПДн, в том числе посредством информационно-телекоммуникационной сети «Интернет», ПДн граждан Российской Федерации должны записываться, систематизироваться, накапливаться, храниться, уточняться (обновляться, изменяться), извлекаться с использованием баз данных, находящихся на территории Российской Федерации.

9.2.4. При сборе ПДн субъекту ПДн по его просьбе необходимо предоставить следующую информацию:

1) подтверждение факта обработки ПДн;

2) правовые основания и цели обработки ПДн;

3) применяемые в Компании способы обработки ПДн;

4) наименование и фактический адрес Компании, сведения о лицах (за исключением работников Компании), которые имеют доступ к ПДн или которым могут

быть раскрыты ПДн на основании договора с оператором или на основании федерального закона;

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

6) сроки обработки ПДн, в том числе сроки их хранения;

7) порядок осуществления субъектом ПДн прав, предусмотренных федеральным законом;

8) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению Компании, если обработка поручена или будет поручена такому лицу.

Предоставления указанных сведений осуществляется в порядке, описанном в документе «Регламент реагирования на запросы субъектов персональных данных».

9.2.5. Если ПДн получены не от субъекта ПДн, то до начала обработки таких ПДн необходимо предоставить субъекту ПДн следующую информацию:

– наименование Компании;

– цель обработки ПДн и ее правовое основание;

– предполагаемые пользователи ПДн;

– права субъекта ПДн, установленные [16.1];

– источник получения ПДн.

Указанная информация может не предоставляться в следующих случаях:

– субъект ПДн уведомлен об осуществлении обработки его ПДн соответствующим оператором;

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

– ПДн сделаны общедоступными субъектом ПДн или получены из общедоступного источника;

– предоставление субъекту ПДн указанных сведений нарушает права и законные интересы третьих лиц.

Порядок и форма предоставления указанной в данном пункте информации описаны в документе «Регламент реагирования на запросы субъектов персональных данных».

9.3. Хранение и учет персональных данных

9.3.1. В Компании должно быть обеспечено раздельное хранение ПДн при разных целях обработки и не допускается на одном бумажном носителе фиксация ПДн, цели обработки которых заведомо несовместимы.

9.3.2. Хранение ПДн в Компании должно осуществляется в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели их обработки и требования нормативных документов РФ, связанных с хранением документов, после чего данные могут быть обезличены (при необходимости).

9.3.3. Порядок учета и хранения носителей ПДн определен в документе «Положение по обеспечению безопасности персональных данных».

9.3.4. Для хранения ПДн на материальных носителях должны использоваться металлические шкафы и сейфы.

9.4. Использование персональных данных

В Компании запрещено принятие на основании исключительно автоматизированной обработки ПДн решений, порождающих юридические последствия в отношении субъекта ПДн или иным образом затрагивающих его права и законные интересы.

9.5. Трансграничная передача персональных данных

В Компании не осуществляется трансграничная передача персональных данных (передача персональных данных на территории иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу).

9.6. Блокирование персональных данных

Компания блокирует обрабатываемые ПДн при выявлении их недостоверности или неправомерных действий в отношении субъекта ПДн в следующих случаях:

– по требованию субъекта ПДн (порядок описан в документе «Регламент реагирования на запросы субъектов персональных данных»);

– по требованию уполномоченного органа по защите прав субъектов ПДн;

– по результатам внутренних контрольных мероприятий (порядок описан в документе «Положение по обеспечению безопасности персональных данных»).

9.7. Уничтожение персональных данных

9.7.1. Компания уничтожает ПДн в случае:

– достижения целей обработки ПДн или утраты необходимости в их достижении;

– получения соответствующего запроса от субъекта ПДн, при условии, что данный запрос не противоречит требованиям законодательства РФ;

– отзыва согласия субъекта на обработку его ПДн (если отзыв согласия влечет за собой уничтожение ПДн);

– получения соответствующего предписания от уполномоченного органа по защите прав субъектов.

9.7.2. Порядок уничтожения ПДн описан в документе «Положение по обеспечению безопасности персональных данных».

9.8. Особенности неавтоматизированной обработки персональных данных

9.8.1. При использовании внутренних типовых форм документов, характер информации в которых предполагает или допускает включение в них ПДн (далее – типовая форма), должны выполняться следующие условия:

– в типовые формы или в связанные с ними документы (инструкция по ее заполнению, карточки, реестры и журналы) включаются сведения о цели обработки ПДн, осуществляемой без использования средств автоматизации, наименование и адрес Компании, фамилия, имя, отчество и адрес субъекта ПДн, источник получения ПДн, сроки обработки ПДн, перечень действий с ПДн, которые будут совершаться в процессе их обработки, общее описание используемых в Компании способов обработки ПДн;

– в случае необходимости получения письменного согласия на обработку ПДн, в типовую форму включается поле, в котором субъект ПДн может поставить отметку о своем согласии на обработку ПДн, осуществляемую без использования средств автоматизации;

– типовая форма составляется таким образом, чтобы каждый из субъектов ПДн, чьи ПДн содержатся в документе, имел возможность ознакомиться со своими ПДн, не нарушая прав и законных интересов иных субъектов ПДн;

– в типовой форме исключается объединение полей, предназначенных для внесения ПДн, цели обработки которых заведомо не совместимы.

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

– необходимость ведения такого журнала (реестра, книги) оформляется приказом, 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 Компании без подтверждения подлинности ПДн, сообщенных субъектом ПДн;

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

– ПДн каждого субъекта могут заноситься в такой журнал (книгу, реестр) не более одного раза в каждом случае пропуска субъекта ПДн на территорию Компании.

10. ОБУЧЕНИЕ РАБОТНИКОВ КОМПАНИИ ПРАВИЛАМ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

10.1. В Компании все работники, участвующие в обработке ПДн, в обязательном порядке должны проходить внутренний инструктаж по следующим темам:

– общие вопросы обеспечения информационной безопасности в Компании;

– правила обработки ПДн;

– правила использования средств защиты информации, входящих в состав СЗПДн Компании;

– ответственность за нарушение правил обработки и обеспечения безопасности ПДн.

Новые работники в обязательном порядке проходят вводный инструктаж по указанным темам.

10.2. Ответственным за организацию проведения инструктажа работников Компании, участвующих в обработке и обеспечении безопасности ПДн, является Ответственный за организацию обработки ПДн. Управление Доступом к персональным данным.

11. УПРАВЛЕНИЕ ДОСТУПОМ РАБОТНИКОВ К ПЕРСОНАЛЬНЫМ ДАННЫМ

11.1. Для определения перечня работников Компании, допущенных к работе с ПДн, разрабатывается и утверждается перечень подразделений и лиц, допущенных к работе с ПДн, в котором указываются структурные подразделения, должности, отдельные лица (при необходимости) и группы ПДн, к работе с которыми они допущены.

11.2. Работник допускается к обработке ПДн только после:

– ознакомления с требованиями настоящего Положения и иными организационно-распорядительными документами на СЗПДн, выполнение требований которых обязательно для соответствующих работников;

– прохождения инструктажа по правилам обработки и обеспечения безопасности ПДн;

– ознакомления с видами ответственности за нарушение установленных в Компании правил обработки и обеспечения безопасности ПДн.

11.3. При получении доступа к ПДн, за работником закрепляется роль Пользователя ПДн.

12. УПРАВЛЕНИЕ ДОСТУПОМ ТРЕТЬИХ СТОРОН К ПЕРСОНАЛЬНЫМ ДАННЫМ

12.1.1. Компания в ходе своей деятельности осуществляет предоставление доступа (в т. ч. осуществляет передачу) к ПДн третьим лицам в целях исполнения договорных обязательств перед субъектами ПДн, а также с целью обеспечения своей деятельности или исполнения требований нормативных документов РФ. При этом субъект ПДн может беспрепятственно получить доступ к перечню третьих сторон, которым предоставляется доступ к его ПДн, если это не противоречит требованиям законодательства РФ.

12.1.2. Компанией передаются ПДн только в объеме, необходимом для достижения заявленных целей обработки.

12.1.3. Существенным условием договоров с третьими сторонами, в рамках исполнения которых предоставляется доступ к ПДн, является обязанность соблюдения сторонами мер обеспечения безопасности ПДн при их обработке. Кроме того, в договорах в обязательном порядке определяется порядок передачи ПДн.

13. ПОРУЧЕНИЕ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

13.1. Компания может поручать обработку ПДн другим лицам (третьим сторонам), а также выступать в роли лица, осуществляющего обработку ПДн по поручению других операторов ПДн.

13.2. Компания поручает обработку ПДн третьим сторонам только с согласия субъекта ПДн или при наличии иного законного основания (договор с субъектом ПДн) при обязательном условии соблюдения стороной, осуществляющей обработку ПДн по поручению Компании, соблюдения правил обработки и обеспечения безопасности ПДн, установленных Компанией.

13.3. При обработке ПДн по поручению третьих сторон Компании соблюдаются установленные соответствующими поручениями (договорами) требования к обеспечению безопасности ПДн.

13.4. В поручении на обработку ПДн должны быть в обязательном порядке определены:

– перечень действий (операций) с ПДн, которые будут совершаться лицом (перечень действий не должен противоречить целям и действиям, заявленным перед субъектом – в договоре, согласии и т. д.);

– цели обработки (цели не должны противоречить целям, заявленным перед субъектом – в договоре, в согласии и т. д.);

– обязанность такого лица соблюдать конфиденциальность ПДн и обеспечивать безопасность ПДн при их обработке;

– требования к защите ПДн (требования по защите, предъявляемые к лицу, осуществляющему обработку, не должны быть выше требований, выполняемых самим оператором – в идеальном случае требования должны быть идентичны).

13.5. Взаимодействие с субъектами персональных данных и органами власти.

14. ВЗАИМОДЕЙСТВИЕ С СУБЪЕКТАМИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Порядок взаимодействия с субъектами ПДн или их законными представителями описан в документе «Регламент реагирования на запросы субъектов персональных данных».

14.1. Взаимодействие с органами власти

14.2. Взаимодействие с органами власти осуществляется в соответствии с законодательством РФ.

14.3. Оценка законности и мотивированности запросов органов власти на предоставление информации о процессах обработки ПДн (в т. ч. на предоставление ПДн) проводится Ответственным за организацию обработки ПДн.

14.4. Подача уведомления о намерении осуществлять обработку ПДн (далее – Уведомление) осуществляется в порядке, предусмотренном в [16.1]. Форма и детальный состав Уведомления определяется в соответствии с нормативными документами Уполномоченного органа по защите прав субъектов ПДн. Ответственным за подачу Уведомления является Ответственный за организацию обработки ПДн.

14.5. Контроль необходимости внесения изменений в Уведомление осуществляется в рамках мероприятий по модернизации и внутреннему контролю СЗПДн, описанных в документе «Положение по обеспечению безопасности персональных данных».

14.6. Уполномоченным органом по защите прав субъектов ПДн (основным регулятором в сфере обработки ПДн) является Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (далее – "Роскомнадзор"). Роскомнадзор, в частности, уполномочен:

– осуществлять проверку сведений, содержащихся в Уведомлении, и привлекать для осуществления такой проверки иные государственные органы в пределах их полномочий;

– обращаться к операторам с требованиями по уточнению, блокированию или уничтожению недостоверных или полученных незаконным путем ПДн;

– принимать в установленном законодательством РФ порядке меры по приостановлению или прекращению обработки ПДн, осуществляемой с нарушением требований [16.1];

– направлять в ФСБ России и ФСТЭК России сведения о мерах по обеспечению безопасности ПДн, указанных в Уведомлении;

– направлять в органы прокуратуры, другие правоохранительные органы материалы для решения вопроса о возбуждении уголовных дел по признакам преступлений, связанных с нарушением прав субъектов персональных данных, в соответствии с подведомственностью;

– привлекать к административной ответственности лиц, виновных в нарушении требований [16.1].

14.7. ФСБ России и ФСТЭК России могут быть наделены решением Правительства РФ полномочиями по контролю за выполнением организационных и технических мер по обеспечению безопасности ПДн, без права ознакомления с ПДн, обрабатываемыми в информационных системах персональных данных. В т. ч. это касается отдельных решений Правительства РФ о проведении контрольных мероприятий.

15. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

15.1. Иные права и обязанности работников, в служебные обязанности которых входит обработка персональных данных, определяются также их должностными инструкциями.

15.2. Лица, виновные в нарушении норм, регулирующих обработку и защиту персональных данных, несут материальную, дисциплинарную, административную, гражданско-правовую или уголовную ответственность в порядке, установленном федеральными законами.

15.3. Разглашение персональных данных, их публичное раскрытие, утрата документов и иных носителей, содержащих персональные данные, а также иные нарушения обязанностей по их защите и обработке, установленных настоящим Положением, другими локальными нормативными актами (приказами, распоряжениями) Компании, влечет наложение на работника, имеющего доступ к персональным данным, дисциплинарного взыскания – замечания, выговора, увольнения.

15.4. Работник, допущенный к обработке персональных данных и совершивший указанный дисциплинарный проступок, несет полную материальную ответственность в

случае причинения его действиями ущерба работодателю (пункт 7 статьи 243 Федерального закона от 30.12.2001 № 197-ФЗ «Трудовой кодекс Российской Федерации»).

15.5. Работники Компании, имеющие доступ к персональным данным, виновные в их незаконном разглашении или использовании без согласия субъектов персональных данных из корыстной или иной личной заинтересованности и причинившие крупный ущерб, несут уголовную ответственность в соответствии со статьей 183 Федерального закона от 13.06.1996 № 63-ФЗ «Уголовный кодекс Российской Федерации».

16. НОРМАТИВНЫЕ ССЫЛКИ

В настоящем Положении использованы ссылки на следующие нормативные правовые акты:

16.1. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

16.2. Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

16.3. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных