|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **РАЗРАБОТЧИК:**   |  |  |  | | --- | --- | --- | | **Должность** | **ФИО** | **Подпись** | | Ведущий специалист по информационной безопасности | Булатова О.А. |  | | **УТВЕРЖДАЮ**  Генеральный директор  \_\_\_\_\_\_\_\_\_\_ А.М. Попова  «\_\_\_\_»\_\_\_\_\_\_\_\_\_\_2020г |
| **Введен в действие**  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  каким документом/ от какого числа  **Сведения о документе** взамен СМК П 45-2018 (версия 2.0)  введен впервые/ взамен (№ и дата предыдущей версии) |

**Содержание:**

[1. НАЗНАЧЕНИЕ И ОБЛАСТЬ ПРИМЕНЕНИЯ 1](#_Toc55907169)

[2. НОРМАТИВНЫЕ ДОКУМЕНТЫ 2](#_Toc55907170)

[3. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ 2](#_Toc55907171)

[4. ОБОЗНАЧЕНИЯ и сокращения 3](#_Toc55907172)

[5. ОБЩИЕ положения 3](#_Toc55907173)

[6. ЦЕЛИ и состав ПЕРСОНАЛЬНЫХ ДАННЫХ 5](#_Toc55907174)

[7. ПОРЯДОК ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ОБЩЕСТВЕ 11](#_Toc55907175)

[8. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОБРАБАТЫВАЕМЫХ В ОБЩЕСТВЕ 11](#_Toc55907176)

[9. ЛИЦА, ОТВЕТСТВЕННЫЕ ЗА ОРГАНИЗАЦИЮ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ОБЩЕСТВЕ 11](#_Toc55907177)

[10. РАССМОТРЕНИЕ ЗАПРОСОВ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ ИЛИ ИХ ПРЕДСТАВИТЕЛЕЙ 14](#_Toc55907178)

[11. РАССМОТРЕНИЕ ЗАПРОСОВ УПОЛНОМОЧЕННЫХ ОРГАНОВ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ 17](#_Toc55907179)

[12. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ НОРМ, РЕГУЛИРУЮЩИХ ОБРАБОТКУ И ЗАЩИТУ ПЕРСОНАЛЬНЫХ ДАННЫХ 17](#_Toc55907180)

[13. ПОРЯДОК ВСТУПЛЕНИЯ В СИЛУ ПОЛОЖЕНИЯ И ВНЕСЕНИЯ ИЗМЕНЕНИЙ 17](#_Toc55907181)

[14. РИСКИ, КОРРЕКТИРУЮЩИЕ И ПРЕДУПРЕЖДАЮЩИЕ МЕРОПРИЯТИЯ 18](#_Toc55907182)

[15. КОНТРОЛЬНЫЕ ТОЧКИ 21](#_Toc55907183)

[СОГЛАСОВАНИЕ 22](#_Toc55907184)

[ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ 22](#_Toc55907185)

[ЛИСТ ОЗНАКОМЛЕНИЯ 23](#_Toc55907186)

1. **НАЗНАЧЕНИЕ И ОБЛАСТЬ ПРИМЕНЕНИЯ**
   1. Положение о персональных данных в АО «Губернские аптеки» (далее – «Положение») определяет цели, принципы обработки персональных данных, содержание, состав персональных данных, обрабатываемых в АО «Губернские аптеки» (далее – Общество).
   2. Требования данного положения распространяются на всех работников Общества.
2. **НОРМАТИВНЫЕ ДОКУМЕНТЫ**

|  |  |
| --- | --- |
| Реквизиты документа | **Название** |
| Принята всенародным голосованием 12.12.1993 | Конституция Российской Федерации |
| № 197-ФЗ от 30.12.2001 | Трудовой кодекс Российской Федерации |
| Федеральный закон № 152-ФЗ от 27.07.2006 | Федеральный закон «О персональных данных» |
| Федеральный закон № 149-ФЗ от 27.07.2006 | Федеральный закон «Об информации, информационных технологиях и о защите информации» |
| Постановление Правительства РФ от 01.11.2012 № 1119 | «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» |
| Постановление Правительства РФ от 15.09.2008 № 687 | «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» |
| Приказ 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 |

1. **ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ**

Для целей настоящего Положения используются следующие основные понятия:

**Работник** — физическое лицо, вступившее в трудовые отношения с Обществом;

**Соискатель –** физическое лицо, претендующее на замещение должности в Обществе;

**Контрагент по договору гражданско-правового характера** – физическое лицо, вступившее в гражданско-правовые отношения с Обществом с целью выполнения определенных работ / оказания услуг;

**Льготополучатель –** физическое лицо, имеющее право на предоставление социальной услуги в части обеспечения необходимыми лекарственными препаратами, изделиями медицинского назначения, а также специализированными продуктами детского питания для детей-инвалидов в соответствии с действующим законодательством;

**Врач** – специалист с высшим медицинским образованием, назначающий лекарственный препарат, изделие медицинского назначения, специализированный продукт детского питания для льготополучателя;

**Покупатель Интернет-магазина** – физическое лицо, посетитель сайта, разместившее заказ в Интернет-магазине;

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

**Общедоступные персональные данные** **-** персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных 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 персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

**Информация** **-** сведения (сообщения, данные) независимо от формы их представления;

**Автоматизированное рабочее место -** это рабочее место, оснащенное персональной ЭВМ, которая на основе использования программного, методического и информационного обеспечения позволяет автоматизировать рабочие процессы;

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

**Интернет-магазин –** информационная система Общества в виде сайта, расположенного в сети Интернет по адресу http://[www.24farmacia.ru](http://www.24farmacia.ru), предназначенная для обработки заказов товаров покупателями.

1. **ОБОЗНАЧЕНИЯ и сокращения**

**ПДн –** персональные данные

**АРМ** – автоматизированное рабочее место

**ИСПДн** - информационная система персональных данных

1. **ОБЩИЕ положения**
   1. Данное Положение разработано с целью обеспечения защиты персональных данных работников, соискателей, контрагентов по договорам гражданско-правового характера, льготополучателей, врачей, покупателей Интернет-магазина и иных категорий граждан в соответствии с требованиями действующего законодательства Российской Федерации.
   2. Виды персональных данных, обрабатываемые в обществе:

* персональные данные работников Общества;
* персональные данные родственников работников Общества;
* персональные данные соискателей;
* персональные данные контрагентов по договорам гражданско-правового характера;
* персональные данные льготополучателей, врачей;
* персональные данные покупателей Интернет-магазина;
* персональные данные иных категорий граждан.
  1. Принципы обработки персональных данных:
* законность целей и способов обработки персональных данных;
* добросовестность деятельности Общества при обработке персональных данных;
* достоверность персональных данных, их достаточность для целей обработки, недопустимость обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;
* обработка только персональных данных, которые отвечают требованиям их обработки;
* недопустимость объединения баз данных, содержащих персональные данные, обработка которых осуществляется в разных целях;
* хранение персональных данных в форме, позволяющей определить субъекта персональных данных.

1. **ЦЕЛИ и состав ПЕРСОНАЛЬНЫХ ДАННЫХ**

| **Категория субъектов персональных данных** | **Цели обработки персональных данных** | **Состав обрабатываемых персональных данных** |
| --- | --- | --- |
| **Персональные данные работников Общества** | Заключение, сопровождение, изменение, расторжение трудовых договоров и соглашений об их расторжении, которые являются основанием для возникновения или прекращения трудовых отношений между работниками и Обществом;  исполнение Обществом обязательств, предусмотренных внутренними нормативно-методическими документами, трудовыми договорами, федеральным законодательством и иными нормативными правовыми актами, в том числе в целях ведения кадрового и бухгалтерского учета, составления налоговой и другой обязательной отчетности;  обучение работников и продвижение по службе;  заключение, изменение, расторжение договоров добровольного медицинского страхования;  организация медицинских осмотров работников;  организационная поддержка командировок и поездок;  оформление пропусков для прохода на территорию Общества;  обеспечение личной безопасности работников, контроля количества и качества выполняемой работниками работы, обеспечения сохранности имущества;  обеспечение социальных гарантий | * + 1. фамилия, имя, отчество (в том числе предыдущие фамилии, имена и (или) отчества, в случае их изменения);     2. число, месяц, год рождения;     3. место рождения;     4. информация о гражданстве (в том числе предыдущие гражданства, иные гражданства);     5. вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи, код подразделения;     6. адрес места жительства (адрес регистрации, фактического проживания);     7. номер контактного телефона или сведения о других способах связи;     8. реквизиты страхового свидетельства государственного пенсионного страхования;     9. идентификационный номер налогоплательщика;     10. реквизиты страхового медицинского полиса обязательного медицинского страхования;     11. реквизиты свидетельства государственной регистрации актов гражданского состояния;     12. семейное положение, состав семьи и сведения о близких родственниках (в том числе бывших);     13. сведения о трудовой деятельности;     14. сведения о воинском учете и реквизиты документов воинского учета;     15. сведения об образовании, в том числе о послевузовском профессиональном образовании (наименование и год окончания образовательного учреждения, наименование и реквизиты документа об образовании, квалификация, специальность по документу об образовании);     16. сведения об ученой степени;     17. информация о владении иностранными языками, степень владения;     18. медицинское заключение по установленной форме об отсутствии у гражданина заболевания, препятствующего замещению должности Общества;     19. фотография;     20. сведения о прежних местах работы;     21. информация, содержащаяся в трудовом договоре, дополнительных соглашениях к трудовому договору;     22. сведения о профессиональной переподготовке и (или) повышении квалификации;     23. информация о ежегодных оплачиваемых отпусках, учебных отпусках и отпусках без сохранения денежного содержания;     24. сведения о доходах, об имуществе и обязательствах имущественного характера;     25. номер расчетного счета;     26. номер банковской карты;     27. иные персональные данные, необходимые для достижения целей |
| **Персональные данные родственников работников Общества** | Исполнение Обществом обязательств, предусмотренных федеральным законодательством (получение алиментов, оформление социальных выплат, пособий) | 1) фамилия, имя, отчество;  2) степень родства;  3) дата рождения;  4) место рождения;  5) место работы;  6) адрес места жительства;  7) сведения о документе, удостоверяющем личность (опционально);  8) банковские реквизиты и суммы перечислений (опционально);  9) иные персональные данные, необходимые для достижения целей |
| **Персональные данные соискателей** | Рассмотрение резюме и подбор кандидатов на вакантную должность для дальнейшего трудоустройства в Общество;  ведение кадрового резерва Общества. | * + 1. фамилия, имя, отчество (в том числе предыдущие фамилии, имена и (или) отчества, в случае их изменения);     2. число, месяц, год рождения (возраст кандидата);     3. информация о гражданстве;     4. вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи, код подразделения;     5. номер контактного телефона или сведения о других способах связи;     6. сведения о трудовой деятельности;     7. сведения об образовании, в том числе о послевузовском профессиональном образовании (наименование и год окончания образовательного учреждения, наименование и реквизиты документа об образовании, квалификация, специальность по документу об образовании);     8. сведения об ученой степени;     9. информация о владении иностранными языками, степень владения;     10. медицинское заключение по установленной форме об отсутствии у гражданина заболевания, препятствующего замещению должности Общества;     11. фотография;     12. сведения о прежних местах работы;     13. сведения о профессиональной переподготовке и (или) повышении квалификации;     14. иные персональные данные, необходимые для достижения цели |
| **Персональные данные контрагентов по договорам гражданско-правового характера** | Согласование условий выполнения работ / оказания услуг контрагентами по договорам гражданско-правового характера;  заключение, изменение, расторжение договоров, а также выполнение обязательств по заключенным договорам;  решение задач финансового и бухгалтерского учета и выполнение операций по налогообложению, правового обеспечения деятельности Общества | * + 1. фамилия, имя, отчество (в том числе предыдущие фамилии, имена и (или) отчества, в случае их изменения);     2. число, месяц, год рождения;     3. место рождения;     4. информация о гражданстве (в том числе предыдущие гражданства, иные гражданства);     5. вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи, код подразделения;     6. адрес места жительства (адрес регистрации, фактического проживания);     7. номер контактного телефона или сведения о других способах связи;     8. реквизиты страхового свидетельства государственного пенсионного страхования;     9. идентификационный номер налогоплательщика;     10. сведения о трудовой деятельности;     11. информация, содержащаяся в договоре гражданско-правового характера, дополнительных соглашениях к нему;     12. сведения о профессиональной переподготовке и (или) повышении квалификации;     13. номер расчетного счета;     14. номер банковской карты;     15. иные персональные данные, необходимые для достижения целей. |
| **Персональные данные льготополучателей**  **Персональные данные врачей** | обеспечение льготополучателей необходимыми лекарственными препаратами, изделиями медицинского назначения, а также специализированными продуктами детского питания для детей-инвалидов в соответствии с действующим законодательством | * + 1. фамилия, имя, отчество (последнее при наличии);     2. адрес места жительства (адрес регистрации, фактического проживания);     3. число, месяц, год рождения;     4. вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи, код подразделения;     5. реквизиты страхового свидетельства государственного пенсионного страхования;     6. реквизиты страхового медицинского полиса обязательного медицинского страхования;     7. сведения об инвалидности, диагнозе, категории заболевания;     8. данные о льготах;     9. иные персональные данные, необходимые для достижения целей     10. фамилия, имя, отчество;     11. место работы;     12. должность;     13. индивидуальный код врача;     14. иные персональные данные, необходимые для достижения целей. |
| **Персональные данные покупателей Интернет-магазина** | обработка запросов на приобретение товаров, размещенных в Интернет-магазине | * + 1. фамилия, имя, отчество (последнее при наличии);     2. адрес доставки;     3. номер телефона;     4. адрес электронной почты;     5. иные персональные данные, необходимые для достижения целей |
| **Персональные данные участников закупок и торгов** | рассмотрение участников закупок и торгов на соответствие требованиям в соответствии с действующим законодательством РФ | * + 1. фамилия, имя, отчество (в том числе предыдущие фамилии, имена и (или) отчества, в случае их изменения);     2. вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи, код подразделения;     3. адрес места жительства (адрес регистрации, фактического проживания);     4. номер контактного телефона или сведения о других способах связи;     5. идентификационный номер налогоплательщика;     6. иные персональные данные, необходимые для достижения целей, указанных в согласии на обработку персональных данных |
| **Персональные данные иных категорий граждан** | цели, указанные в письменном согласии на обработку персональных данных | * + 1. фамилия, имя, отчество (в том числе предыдущие фамилии, имена и (или) отчества, в случае их изменения);     2. число, месяц, год рождения;     3. место рождения;     4. информация о гражданстве (в том числе предыдущие гражданства, иные гражданства);     5. вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи, код подразделения;     6. адрес места жительства (адрес регистрации, фактического проживания);     7. номер контактного телефона или сведения о других способах связи;     8. иные персональные данные, необходимые для достижения целей, указанных в согласии на обработку персональных данных |
| **Персональные данные иных категорий граждан** | соблюдение действующего законодательства Российской Федерации | * + 1. фамилия, имя, отчество (в том числе предыдущие фамилии, имена и (или) отчества, в случае их изменения);     2. число, месяц, год рождения;     3. место рождения;     4. информация о гражданстве (в том числе предыдущие гражданства, иные гражданства);     5. вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи, код подразделения;     6. адрес места жительства (адрес регистрации, фактического проживания);     7. номер контактного телефона или сведения о других способах связи;     8. иные персональные данные, необходимые для достижения цели |

1. **ПОРЯДОК ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ОБЩЕСТВЕ**
   1. Обработка персональных данных в Обществе осуществляется в соответствии с «Положением об обработке персональных данных», утвержденным приказом генерального директора.
2. **ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОБРАБАТЫВАЕМЫХ В ОБЩЕСТВЕ**
   1. Обеспечение безопасности персональных данных, обрабатываемых в информационных системах персональных данных Общества, достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, а также принятия следующих мер по обеспечению безопасности:
   2. определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных Общества;
   3. применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Общества, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;
   4. применение прошедших в установленном порядке процедур оценки соответствия средств защиты информации;
   5. оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
   6. учет машинных носителей персональных данных;
   7. обнаружение фактов несанкционированного доступа к персональным данным и принятие мер по предотвращению несанкционированного доступа;
   8. восстановление персональных данных, модифицированных или удаленных, уничтоженных вследствие несанкционированного доступа к ним;
   9. установление правил доступа к персональным данным, обрабатываемым в информационных системах персональных данных Общества, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационных системах персональных данных Общества;
   10. контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровней защищенности информационных систем персональных данных.
3. **ЛИЦА, ОТВЕТСТВЕННЫЕ ЗА ОРГАНИЗАЦИЮ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ОБЩЕСТВЕ**
   1. Ответственные за организацию обработки персональных данных в Обществе назначаются генеральным директором в соответствии с распределением обязанностей. Ответственные за обработку персональных данных в своей работе руководствуются законодательством Российской Федерации в области персональных данных, настоящим Положением и иными локальными нормативными актами Общества.
   2. Ответственные за обработку персональных данных обязаны:
      1. организовывать принятие правовых, организационных и технических мер для обеспечения защиты персональных данных, обрабатываемых в Обществе от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных;
      2. осуществлять внутренний контроль за соблюдением работниками Общества требований законодательства Российской Федерации в области персональных данных, в том числе требований к защите персональных данных;
      3. доводить до сведения работников Общества положения законодательства Российской Федерации в области персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;
      4. организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей, а также осуществлять контроль за приемом и обработкой таких обращений в Обществе;
      5. в случае если Общество пользуется услугами контрагентов на основании заключенных договоров (либо иных оснований), и в силу данных договоров им передаются персональные данные или поручается обработка персональных данных, инициировать и контролировать включение в договоры пунктов, содержащих:
         * перечень действий с персональными данными и цели обработки;
         * обязанность контрагента соблюдать конфиденциальность персональных данных и обеспечивать их безопасность при обработке;
         * требования к защите обрабатываемых персональных данных.
      6. поддерживать формы согласий субъектов в актуальном состоянии, в том числе контролировать внесение в формы согласий наименование контрагентов, которым передаются персональные данные или которым поручается обработка персональных данных;
      7. в случае нарушения в Обществе требований к защите персональных данных принимать необходимые меры по восстановлению нарушенных прав субъектов персональных данных и разрабатывать предложения по устранению недостатков и предупреждению подобного рода нарушений.
   3. Ответственные за обработку персональных данных вправе:
      1. иметь доступ к информации, касающейся обработки персональных данных в обществе и включающей:
         * цели обработки персональных данных;
         * категории обрабатываемых персональных данных;
         * категории субъектов, персональные данные которых обрабатываются;
         * правовые основания обработки персональных данных;
         * перечень действий с персональными данными, общее описание в Обществе способов обработки персональных данных;
         * описание мер, предусмотренных [статьями 18.1](consultantplus://offline/ref=72A526DC4172CA948EBA325BF95ABE0FBB1E9A61EED0A9056E06BC651C27B3E668EB97CB24EABA22ECx2C) и [19](consultantplus://offline/ref=72A526DC4172CA948EBA325BF95ABE0FBB1E9A61EED0A9056E06BC651C27B3E668EB97CB24EABA21ECxDC) Федерального закона «О персональных данных», в том числе сведения о наличии шифровальных (криптографических) средств и наименования этих средств;
         * дату начала обработки персональных данных;
         * срок или условия прекращения обработки персональных данных;
         * сведения о наличии или об отсутствии трансграничной передачи персональных данных в процессе их обработки;
         * сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством Российской Федерации;
      2. привлекать к реализации мер, направленных на обеспечение безопасности персональных данных, обрабатываемых в Обществе, иных работников Общества с возложением на них соответствующих обязанностей и закреплением ответственности.
   4. Ответственные за обработку персональных данных в Обществе несут ответственность за надлежащее выполнение возложенных функций по организации обработки персональных данных в Обществе в соответствии с положениями законодательства Российской Федерации в области персональных данных.
   5. Структурное подразделение Общества, ответственное за обеспечение информационной безопасности в Обществе (отдел информационно-технического сопровождения), организует и контролирует ведение учета материальных носителей персональных данных.
   6. Отдел информационно-технического сопровождения должен обеспечить:
      1. своевременное обнаружение фактов несанкционированного доступа к персональным данным и немедленное доведение этой информации до ответственного за организацию обработки персональных данных в Обществе и генерального директора;
      2. недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;
      3. возможность восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
      4. постоянный контроль за обеспечением уровня защищенности персональных данных;
      5. знание и соблюдение условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;
      6. учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;
      7. при обнаружении нарушений порядка предоставления персональных данных незамедлительное приостановление предоставления персональных данных пользователям информационной системы персональных данных до выявления причин нарушений и устранения этих причин;
      8. разбирательство и составление заключений по фактам несоблюдения условий хранения материальных носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений.
   7. Отдел информационно-технического сопровождения принимает все необходимые меры по восстановлению персональных данных, модифицированных или удаленных, уничтоженных вследствие несанкционированного доступа к ним.
   8. В случае выявления нарушений порядка обработки персональных данных в информационных системах персональных данных Общества уполномоченными должностными лицами незамедлительно принимаются меры по установлению причин нарушений и их устранению.
4. **РАССМОТРЕНИЕ ЗАПРОСОВ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ ИЛИ ИХ ПРЕДСТАВИТЕЛЕЙ**
   1. Субъекты персональных данных, данные которых обрабатываются Обществом, имеют право на получение информации, касающейся обработки их персональных данных, в том числе содержащей:
      * подтверждение факта обработки персональных данных в Обществе;
      * правовые основания и цели обработки персональных данных;
      * применяемые в Обществе способы обработки персональных данных;
      * наименование и место нахождения Общества, сведения о лицах, которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Обществом или на основании федерального закона;
      * обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
      * сроки обработки персональных данных, в том числе сроки их хранения в Обществе;
      * порядок осуществления субъектом персональных данных прав, предусмотренных законодательством Российской Федерации в области персональных данных;
      * информацию об осуществленной или предполагаемой трансграничной передаче данных;
      * наименование организации или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Общества, если обработка поручена или будет поручена такой организации или лицу;
      * иные сведения, предусмотренные законодательством Российской Федерации в области персональных данных.
   2. Общество обязано сообщить субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя либо в течение тридцати дней с даты получения запроса субъекта персональных данных или его представителя.
   3. Субъекты персональных данных вправе требовать от Общества уточнения их персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.
   4. В срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, Общество обязано внести в них необходимые изменения. В срок, не превышающий семи 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, Общество обязано уничтожить такие персональные данные. Общество обязано уведомить субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.
   5. Сведения, указанные в [пункте 10.1](#Par316) настоящего Положения, должны быть предоставлены субъекту персональных данных оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.
   6. Сведения, указанные в [пункте 10.1](#Par316) настоящего Положения, предоставляются субъекту персональных данных или его представителю уполномоченным должностным лицом структурного подразделения Общества, осуществляющего обработку соответствующих персональных данных при обращении либо при получении запроса субъекта персональных данных или его представителя. 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 правоотношениях с Обществом, либо сведения, иным образом подтверждающие факт обработки персональных данных Обществом, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с [законодательством](consultantplus://offline/ref=72A526DC4172CA948EBA325BF95ABE0FBB109361EADAA9056E06BC651CE2x7C) Российской Федерации.
   7. В случае если сведения, указанные в  [пункте 10.1](#Par316) настоящего Положения, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно в Общество или направить повторный запрос в целях получения указанных сведений и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, 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 персональных данных.
   8. Субъект персональных данных вправе обратиться повторно в Общество или направить повторный запрос в целях получения сведений, указанных в [пункте 10.1](#Par316) настоящего Положения, а также в целях ознакомления с обрабатываемыми персональными данными, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в [пункте 10.4](#Par319) настоящего Положения, должен содержать обоснование направления повторного запроса.
   9. Общество вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным [пунктами 10.5](#Par322) и [10.6](#Par323) настоящего Положения. Такой отказ должен быть мотивированным.
   10. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами, в том числе если доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц.
   11. Все запросы или обращения должны быть переданы ответственному за организацию обработки персональных данных не позднее дня, следующего за днем их поступления независимо от места подачи. Для этого:
       * работники Общества, обращающиеся за разъяснением об обработке их персональных данных, передают свое обращение руководителю своего подразделения либо в случае его отсутствия непосредственно ответственному за организацию обработки персональных данных;
       * работники Общества, принявшие обращение от иных лиц, передают поступившее обращение руководителю своего подразделения либо в случае его отсутствия непосредственно ответственному за организацию обработки персональных данных в течение 3 часов после поступления обращения;
       * руководители подразделений передают обращение ответственному за организацию обработки персональных данных в течение 1 часа после поступления обращения.
   12. Ответственный за организацию обработки персональных данных после регистрации обращения:
       * рассматривает обращение по существу, привлекая в случае необходимости работников любых подразделений Общества;
       * запрашивает первичные документы и пояснения (в том числе письменные объяснения) работников по существу обращения (срок предоставления – 1 рабочий день). Руководители структурных подразделений несут ответственность за своевременность и полноту предоставления сведений ответственному за организацию обработки персональных данных;
       * при необходимости инициирует и контролирует внесение необходимых изменений в персональные данные субъекта либо их удаление.
   13. Не позднее двух рабочих дней со дня регистрации обращения ответственный за организацию обработки персональных данных готовит ответ на обращение и, при необходимости, согласовывает ответ с руководителем юридического департамента.
   14. Подготовленный и согласованный ответ вместе со всеми имеющимися материалами ответственный за организацию обработки персональных данных передает на подпись генеральному директору Общества.
   15. Подписанный генеральным директором Общества ответ на обращение отправляется субъекту заказным письмом или передается субъекту лично под подпись.
   16. В случае отказа в предоставлении информации субъекту персональных данных при получении обращения ответственный за организацию обработки персональных данных готовит в письменной форме мотивированный ответ, содержащий ссылку на положение части 5 статьи 14 Федерального закона Российской Федерации № 152-ФЗ «О персональных данных» или иного федерального закона, являющегося основанием для такого отказа, в срок не превышающий семи рабочих дней с момента получения обращения субъекта персональных данных. Данный ответ подлежит обязательному согласованию с руководителем юридического департамента.
5. **РАССМОТРЕНИЕ ЗАПРОСОВ УПОЛНОМОЧЕННЫХ ОРГАНОВ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ** 
   1. Запрос уполномоченного органа может быть направлен в электронной форме и подписан электронной подписью в соответствии с законодательством РФ.
   2. После регистрации запроса ответственный за организацию обработки ПДн:
      * рассматривает запрос по существу, привлекая в случае необходимости работников любых подразделений Общества;
      * запрашивает первичные документы и пояснения (в том числе письменные объяснения) работников по существу запроса (срок предоставления – 1 рабочий день). Руководители структурных подразделений несут ответственность за своевременность и полноту предоставления сведений Ответственному за организацию обработки персональных данных;
      * при необходимости инициирует и контролирует внесение необходимых изменений в персональные данные субъектов либо их удаление.
   3. В ответе должны быть освещены все поднятые в запросе вопросы и приложены все требуемые документы. Ответ на запрос должен быть подписан генеральным директором Общества. Подписанный ответ высылается в адрес надзорного органа почтой либо курьерской службой.
6. **ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ НОРМ, РЕГУЛИРУЮЩИХ ОБРАБОТКУ И ЗАЩИТУ ПЕРСОНАЛЬНЫХ ДАННЫХ**
   1. Работники, ответственные за обработку персональных данных в Обществе, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с действующим законодательством и локальными нормативными актами Общества.
7. **ПОРЯДОК ВСТУПЛЕНИЯ В СИЛУ ПОЛОЖЕНИЯ И ВНЕСЕНИЯ ИЗМЕНЕНИЙ**
   1. Настоящее Положение вступает в силу с момента его утверждения генеральным директором Общества и действует бессрочно, до утверждения новой версии Положения либо его отмены.
   2. Изменения в Положение вносятся приказом генерального директора.
   3. Работники Общества должны быть ознакомлены с Положением под роспись.
8. **­РИСКИ, КОРРЕКТИРУЮЩИЕ И ПРЕДУПРЕЖДАЮЩИЕ МЕРОПРИЯТИЯ**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№ п/п** | **Риск** | **Вероятное последствие** | **Предупреждающее мероприятие, направленное на снижение риска (систематические мероприятия для предотвращения возникновения риска)** | **Корректирующее действие (действия в случае возникновения риска)** |
| 1 | Обработка персональных данных без согласия субъекта персональных данных, когда оно требуется, или с согласия, но с неполными сведениями | Административная ответственность за нарушение правил обработки персональных данных | Ежегодная актуализация ответственным за обработку персональных данных форм согласий субъектов персональных данных  Проведение ответственным за безопасность персональных данных внутреннего периодического контроля | Ответственному за обработку персональных данных организовать сбор согласия субъекта персональных данных на обработку персональных данных |
| 2 | Обработка персональных данных в целях, несовместимых с целями сбора | Административная ответственность за нарушение правил обработки персональных данных | Проведение ответственным за безопасность персональных данных внутреннего периодического контроля | Ответственному за обработку персональных данных организовать пересмотр целей обработки персональных данных |
| 3 | Передача персональных данных без наличия законных оснований или согласия субъекта персональных данных | Административная ответственность за нарушение правил обработки персональных данных | Проведение ответственным за безопасность персональных данных внутреннего периодического контроля | Получить согласие субъекта персональных данных на передачу персональных данных |
| 4 | Несанкционированный доступ к обрабатываемой в ИСПДн информации | Административная ответственность за невыполнение требований по защите персональных данных | Проведение ответственным за безопасность персональных данных внутреннего оперативного контроля  Ежедневный мониторинг администратором безопасности средств защиты от несанкционированного доступа | Ответственному за обеспечение безопасности персональных данных организовать служебное расследование инцидента и устранение последствий несанкционированного доступа |
| 5 | Несанкционированный доступ в помещения, где осуществляется обработка персональных данных | Административная ответственность за невыполнение требований по защите персональных данных | Проведение ответственным за безопасность персональных данных внутреннего периодического контроля | Ответственному за обеспечение безопасности персональных данных организовать служебное расследование инцидента и устранение последствий несанкционированного доступа |
| 6 | Непредоставление в определенный срок субъекту персональных данных запрошенную им информацию | Административная ответственность за неисполнение обязанностей при взаимодействии с субъектами персональных данных | Контроль за приемом и обработкой обращений и запросов субъектов персональных данных | Ответственному за обеспечение безопасности персональных данных организовать служебное расследование нарушения и устранение последствий |
| 7 | Непредоставление в срок информации, запрошенную уполномоченным органом по защите персональных данных | Административная ответственность за неисполнение обязанностей при взаимодействии с уполномоченными органами по защите персональных данных | Контроль за приемом и обработкой запросов уполномоченных органов | Ответственному за обеспечение безопасности персональных данных организовать служебное расследование нарушения и устранение последствий |
| 8 | Отсутствие осведомленности сотрудников Общества, допущенных к работе с ПДн | Нарушение законодательных, нормативных или договорных требований | Контроль ответственным за обработку персональных данных проведения инструктажа по вопросам обеспечения безопаности ПДн  Первичный инструктаж перед началом работы в ИСПдн новых сотрудников Общества  Ежегодный повторный инструктаж пользователей ИСПДн  Проверка знаний пользователями ИСПдн положений нормативной документации по вопросам обеспечения безопасности ПДн на Корпоративном портале | Проведение ответственным за обработку персональных данных внепланового повторного инструктажа пользователей ИСПДн |

1. **КОНТРОЛЬНЫЕ ТОЧКИ**

|  |  |  |
| --- | --- | --- |
| **Контрольная точка** | **Ответственный** | **Периодичность** |
| Контроль актуальности форм согласий субъектов персональных данных | Ответственный за обработку персональных данных | Ежегодно либо при существенном изменении процессов обработки персональных данных |
| Внутренний контроль за соблюдением требований законодательства в области персональных данных | Ответственный за обработку персональных данных | Ежегодно |
| Инструктаж пользователей информационных систем персональных данных | Ответственный за обработку персональных данных | Ежегодно |
| Контроль за приемом и обработкой обращений и запросов субъектов персональных данных | Ответственный за обработку персональных данных | Еженедельно |

**СОГЛАСОВАНИЕ**

Согласование в СЭД. Лист согласования формируется автоматически.

**ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ**

| Версия | Дата | Автор | Содержание изменения |
| --- | --- | --- | --- |
| 2.0 |  | Кочеткова С.И. | Актуализация в связи реорганизацией |
| 3.0 |  | Булатова О.А. | Документ оформлен согласно нового шаблона. Дополнены цели обработки персональных данных по категориям субъектов персональных данных.  Уточнен раздел 10 Рассмотрение запросов субъектов персональных данных или их представителей  Добавлен раздел 11 Рассмотрение запросов уполномоченных органов по защите персональных данных.  Добавлен раздел Риски, корректирующие и предупреждающие мероприятия.  Добавлен раздел Контрольные точки. |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**ЛИСТ ОЗНАКОМЛЕНИЯ**

| № п/п | Должность сотрудника | Ф.И.О. | личная подпись | дата ознакомления |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |