**Общество с ограниченной ответственностью**

**«Ромашка»**

УТВЕРЖДАЮ

Руководитель

ООО «Ромашка»

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ И.И.Васильков

\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_201\_\_ г.

**Положение о порядке обработки персональных данных**

**в ООО "Ромашка".**

**Дата введения \_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Издание №\_\_\_**

Настоящий документ не может быть полностью или частично воспроизведен, тиражирован и распространен без разрешения ООО «Ромашка»

2017

ИНФОРМАЦИОННЫЕ ДАННЫЕ

ВВЕДЕНО В ДЕЙСТВИЕ ПРИКАЗОМ №\_\_\_\_\_\_ от \_\_\_\_\_\_\_\_\_20\_\_г.

РАЗРАБОТАНО: Отдел защиты информации

ИСПОЛНИТЕЛИ:

Начальник отдела защиты информации Параноиков А.Е. \_\_\_\_\_\_\_\_

СОГЛАСОВАНО:

Директор департамента ИТ Аникеев Б.Б. \_\_\_\_\_\_\_\_

Начальник юридической службы Палкин П.В. \_\_\_\_\_\_\_\_

Директор финансового департамента Копалкин В.П. \_\_\_\_\_\_\_\_

**СОДЕРЖАНИЕ**

[1. ОСНОВНЫЕ ПОНЯТИЯ 4](#_Toc475953025)

[2. ОСНОВНЫЕ ПОЛОЖЕНИЯ 7](#_Toc475953026)

[3. ЦЕЛЬ И СОДЕРЖАНИЕ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ 9](#_Toc475953027)

[4. ПРИНЦИПЫ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 13](#_Toc475953028)

[5. ПРАВИЛА РАБОТЫ С ОБЕЗЛИЧЕННЫМИ ДАННЫМИ 19](#_Toc475953029)

[6. ПЕРЕДАЧА ПЕРСОНАЛЬНЫХ ДАННЫХ ТРЕТЬИМ ЛИЦАМ 20](#_Toc475953030)

[7. ПРАВА СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ 22](#_Toc475953031)

[8. ПОРЯДОК ДЕЙСТВИЙ ПРИ ПОЛУЧЕНИИ ЗАПРОСОВ НАДЗОРНЫХ ОРГАНОВ 23](#_Toc475953032)

[9. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ СУБЪЕКТОВ 24](#_Toc475953033)

[10. ОБЯЗАННОСТИ ЛИЦ, ДОПУЩЕННЫХ К ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ 26](#_Toc475953034)

[11. ОТВЕТСТВЕННОСТЬ РАБОТНИКА ЗА НАРУШЕНИЕ НОРМ, РЕГУЛИРУЮЩИХ ОБРАБОТКУ И ЗАЩИТУ ПЕРСОНАЛЬНЫХ ДАННЫХ СУБЪЕКТОВ 27](#_Toc475953035)

[12. НОРМАТИВНЫЕ ССЫЛКИ 28](#_Toc475953036)

[Приложение №1 30](#_Toc475953037)

[Приложение №2 38](#_Toc475953038)

[Приложение №3 40](#_Toc475953039)

[Приложение №4 41](#_Toc475953040)

[Приложение №5 42](#_Toc475953041)

[Приложение №6 43](#_Toc475953042)

[Приложение №7 45](#_Toc475953043)

[Приложение №8 47](#_Toc475953044)

[Приложение №9 51](#_Toc475953045)

[Приложение №10 53](#_Toc475953046)

# ОСНОВНЫЕ ПОНЯТИЯ

Для целей настоящего Положения используются следующие основные понятия:

* 1. **Автоматизированная обработка персональных данных** – обработка персональных данных с помощью средств вычислительной техники;
	2. **Безопасность персональных данных** – состояние защищенности персональных данных, при котором обеспечиваются их конфиденциальность, доступность и целостность при их обработке в информационных системах персональных данных;
	3. **Блокирование персональных данных** – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);
	4. **Информационная система персональных данных** – совокупность содержащихся в базах данных персональных данных, и обеспечивающих их обработку информационных технологий и технических средств;
	5. **Конфиденциальность персональных данных** – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания;
	6. **Несанкционированный доступ (несанкционированные действия)** – доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своим функциональному предназначению и техническим характеристикам;
	7. **Обработка персональных данных** – любое действие (операция) или совокупность действий, 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 (в том числе распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;
	8. **Обезличивание персональных данных** – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;
	9. **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;
	10. **Персональные данные** – любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных);
	11. **Предоставление персональных данных** – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;
	12. **Распространение персональных данных** – действия, направленные на раскрытие персональных данных неопределенному кругу лиц;
	13. **Технические средства информационной системы персональных данных**– средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации;
	14. **Трансграничная передача персональных данных** – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу;
	15. **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;
	16. **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.

# ОСНОВНЫЕ ПОЛОЖЕНИЯ

* 1. Цель разработки настоящего Положения – обеспечение защиты прав и свобод человека и гражданина, при обработке его персональных данных, в том числе права на неприкосновенность частной жизни, личную и семейную тайну, а также установление ответственности должностных лиц, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.
	2. Положение разработано в соответствии с Политикой информационной безопасности ООО «Ромашка».
	3. Положение устанавливает порядок обработки персональных данных субъектов ООО «Ромашка» (далее – Общество).
	4. Положение определяет необходимый минимальный объем мер, соблюдение которых позволяет предотвратить утечку сведений, относящихся к персональным данным. При необходимости могут быть введены дополнительные меры, направленные на усиление защиты персональных данных.
	5. Деятельность по организации обработки и защиты персональных данных в соответствии с требованиями законодательства Российской Федерации о персональных данных осуществляет работник или подразделение Общества, назначенные ответственным за организацию обработки персональных данных Общества. Ответственность за организацию обработки персональных данных может быть возложена на ответственного[[1]](#footnote-1) за защиту информации в Обществе. Типовая должностная инструкция ответственного за организацию обработки персональных данных приведена в приложении №10 к настоящему положению.
	6. Деятельность по администрированию средств и механизмов защиты осуществляет ответственный за защиту информации в Обществе.
	7. Техническое обслуживание информационных систем персональных данных осуществляет ответственный за эксплуатацию информационных систем Общества.
	8. Ответственный за организацию обработки персональных данных назначается приказом руководителя Общества.
	9. На основании договора Общество может поручать обработку персональных данных третьим лицам. Лицо, осуществляющее обработку персональных данных по поручению Общества, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом РФ от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ). В поручении Общества, должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со статьей 19 Федерального закона № 152-ФЗ. Типовая форма поручения определена в приложении №9 к настоящему положению.
	10. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьей 24 Конституции Российской Федерации, Общество вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия.
	11. Общество не имеет права получать и обрабатывать персональные данные субъекта о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законодательством Российской Федерации.
	12. Настоящее Положение вступает в силу с момента его утверждения и действует до замены его новым Положением.
	13. Все изменения в Положение вносятся приказом руководителя Общества.

# ЦЕЛЬ И СОДЕРЖАНИЕ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

* 1. Целями обработки персональных данных являются:
* организация пропускного режима на территории Общества;
* организация учета работников Общества для обеспечения соблюдения требований законодательства Российской Федерации и иных нормативно-правовых актов, регулирующих трудовые отношения, содействия в трудоустройстве, обучении, продвижении по службе, пользования различного вида льготами в соответствии с Трудовым кодексом Российской Федерации, Налоговым кодексом Российской Федерации, федеральными законами Российской Федерации, в частности: «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования», «О персональных данных», а также Учредительными документами и нормативными актами Общества;
* исполнение договоров.
	1. Цель «организация пропускного режима на территории Общества» достигается посредством обработки персональных данных граждан:
* фамилия, имя, отчество,
* год рождения,
* паспортные данные.
	1. Цель «обработка в соответствии с трудовым законодательством» достигается посредством обработки персональных данных следующих категорий для следующих субъектов:
1. субъекты, направившие резюме:
* фамилия, имя, отчество,
* место рождения,
* трудоспособность,
* профессия,
* сведения об образовании,
* дата рождения,
* контактные сведения,
* информация о трудовой деятельности,
* адреса регистрации и проживания.
1. собственные работники:
* фамилия, имя, отчество,
* место рождения,
* состав семьи,
* возраст членов семьи;
* трудоспособность,
* сведения о состоянии здоровья;
* семейное положение,
* профессия,
* сведения об образовании,
* дата рождения,
* сведения о воинском учёте,
* контактные сведения,
* информация о трудовой деятельности,
* гражданство,
* паспортные данные,
* социальное положение,
* адреса регистрации и проживания,
* доходы,
* имущественное положение.
1. члены семей работников:
* дата рождения;
* сведения о трудовой деятельности;
* сведения об отнесении к льготной категории граждан.
1. уволенные (уволившиеся) работники:
* фамилия, имя, отчество,
* место рождения,
* состав семьи,
* трудоспособность,
* семейное положение,
* профессия,
* сведения об образовании,
* дата рождения,
* сведения о воинском учёте,
* контактные сведения,
* информация о трудовой деятельности,
* гражданство,
* паспортные данные,
* социальное положение,
* адрес,
* доходы за период трудовых отношений,
* сведения об имущественном положении в период трудовых отношений.
	1. Цель «исполнение договоров» достигается посредством обработки персональных данных следующих категорий для следующих субъектов:
1. клиенты:
* фамилия, имя, отчество,
* контактные сведения,
* паспортные данные,
* сведения о состоянии здоровья.
1. граждане, работники подрядных организаций:
* паспортные данные;
	1. В Обществе предусмотрены следующие формы фиксации персональных данных:
1. граждане, получающие пропуск на территорию Общества:
* заявка на получение пропуска;
* копии документов, удостоверяющих личность;
* пропуск
1. субъекты, направившие резюме:
* резюме;
* анкета соискателя.
1. собственные работники:
* заявление о приеме на работу;
* первичные бухгалтерские документы (заявления работника);
* копии документов, удостоверяющих личность;
* оригиналы документов подтверждающих трудовую деятельность;
* копии документов, подтверждающих образование;
* копии документов о постановке на налоговый учет;
* копии документов о постановке на воинский учет;
* копии документов, подтверждающих право управления транспортным средством;
* личная карточка работника (унифицированные формы Т-1 и Т-2);
* реестр на открытие зарплатных счетов и выпуск пластиковых карт;
* табель учета рабочего времени;
* доверенности на совершение юридически значимых действий от лица Общества;
* справка-резюме для аттестации работника;
* поименные списки на медицинский осмотр;
* заключительные акты медицинского осмотра;
* пропуск;
* карты специальной оценки условий труда;
1. члены семей работников:
* копии свидетельств о рождении;
* копии свидетельств о заключении брака;
* справки с места работы супругов;
* справки из налоговых органов;
* справки об отнесении к льготной категории граждан;
1. граждане, работники подрядных организаций:
* доверенности на совершение юридически значимых действий от лица подрядчика.

# ПРИНЦИПЫ БЕЗОПАСНОЙ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

* 1. Все персональные данные субъектов Общество получает от них самих либо от их законных представителей.
	2. Персональные данные работников (членов их семей) должны быть получены непосредственно от самих работников. Привлечение посредников не допускается.
	3. Обработка персональных данных осуществляется в соответствии с действующим законодательством Российской Федерации на основании согласия субъекта персональных данных, кроме случаев, предусмотренных Федеральным законом № 152-ФЗ. Формы письменного согласия на обработку персональных данных приведены в приложении №1 к настоящему Положению.
	4. Согласие на обработку персональных данных может быть получено также в виде акцепта публичной оферты, размещённой на официальном информационном ресурсе Общества в информационно-телекоммуникационных сетях. Такая форма согласия возможна, если субъект предоставляет свои персональные данные посредством информационно-телекоммуникационных сетей (через официальные публичные информационные ресурсы Общества).
	5. Субъект персональных данных принимает решение о предоставлении своих персональных данных и дает согласие на их обработку своей волей и в своем интересе.
	6. Получение персональных данных субъекта у третьих лиц, возможно только при уведомлении субъекта об этом заранее и с его письменного согласия. Форма согласия приведена в приложении №2 к настоящему Положению.
	7. Персональные данные обрабатываются в структурных подразделениях Общества в соответствии с исполняемыми функциями.
	8. Доступ к персональным данным, обрабатываемым без использования средств автоматизации, осуществляется в соответствии с перечнем должностей, утвержденным руководителем Общества.
	9. Доступ к персональным данным, обрабатываемым в информационных системах персональных данных (далее - ИСПДн), осуществляется в соответствии с перечнем должностей, утвержденным руководителем Общества.
	10. Списочный состав работников Общества, в том числе при составлении списков подразделений, допустимо формировать только на основе существующих в Обществе информационных систем и связанных с ними баз данных, предназначенных для кадрового учета работников Общества, путем выборки из этих баз данных. Создание иных информационных систем и баз данных для ведения списков работников не допускается. Дополнительный сбор персональных данных лицами, не отвечающими за ведение баз данных кадрового учета, не допускается. Отдел кадров обязан обеспечить необходимую полноту баз данных кадрового учета, в том числе наличие в них необходимых контактных данных работников.
	11. Списочный состав членов семей работников Общества, в том числе при составлении списков на получение новогодних подарков, участия в спортивных, творческих и иных мероприятиях допустимо формировать только на основе существующих в Обществе информационных систем и связанных с ними баз данных, предназначенных для кадрового учета работников Общества, путем выборки из этих баз данных. Создание иных информационных систем и баз данных для ведения списков членов семей работников не допускается. Дополнительный сбор персональных данных лицами, не отвечающими за ведение баз данных кадрового учета, не допускается. Отдел кадров обязан обеспечить необходимую полноту баз данных кадрового учета, в том числе наличие в них необходимых сведений о членах семей работников.
	12. Актуализация перечней, указанных в п.п. 4.8, 4.9 выполняется в случае изменения штатного состава или изменения должностных обязанностей лиц, учувствовавших в обработке персональных данных. Актуализация выполняется не реже одного раза в год. Проекты приказов на утверждение или изменение указанных списков готовит начальник отдела кадров.
	13. Уполномоченные лица, допущенные к персональным данным, имеют право получать только те персональные данные субъекта, которые необходимы для выполнения конкретных функций, в соответствии с должностной инструкцией уполномоченных лиц.
	14. Обработка персональных данных, осуществляемая без использования средств автоматизации, должна выполняться в соответствии с требованиями "Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации" утвержденного постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687.

Персональные данные при такой их обработке, должны обособляться от иной информации, в частности, путем фиксации их на отдельных материальных носителях персональных данных, в специальных разделах или на полях форм (бланков).

* 1. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки.
	2. Персональные данные подлежат уничтожению либо обезличиванию в следующих случаях:
1. достижения целей обработки или в случае утраты необходимости в их достижении;
2. отзыва согласия субъекта персональных данных на обработку персональных данных;
3. представления субъектом персональных данных или его законным представителем сведений, подтверждающих, что персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки;
4. выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его законного представителя и невозможности обеспечить правомерную обработку персональных данных.
	1. Для подготовки организационных решений в области обработки и защиты персональных данных в Обществе, приказом руководителя Общества, назначается постоянно действующая экспертная комиссия по защите информации (далее – ПДК ЗИ). Рекомендуется включать в состав ПДК ЗИ не менее одного работника из подразделения, отвечающего за правовое сопровождение деятельности Общества, и не менее одного работника из подразделения, отвечающего за эксплуатацию инфраструктурных объектов информационных систем. Председатель комиссии должен иметь полное понимание структуры бизнес-процессов Общества затрагивающих обработку персональных данных. В состав комиссии в обязательном порядке должен быть включён ответственный за организацию обработки персональных данных в Обществе. Состав комиссии должен пересматриваться не реже одного раза в год.
	2. Хранение материальных носителей персональных данных осуществляется в специально оборудованных шкафах и сейфах. Места хранения определяются в соответствии со списком, утвержденным руководителя Общества. Пересмотр списка выполняется не реже одного раза в год. Проект приказов на утверждение и изменение списка готовит ПДК ЗИ.
	3. Перечень лиц, ответственных за безопасное хранение персональных данных в местах хранения утверждается приказом руководителя Общества. Пересмотр перечня выполняется не реже одного раза в год. Проекты приказов на утверждение и изменение перечня готовит ПДК ЗИ.
	4. В срок, не превышающий 7 рабочих дней со дня предоставления субъектом персональных данных или его законным представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, Общество вносит в них необходимые изменения, а также уведомляет субъект о внесенных изменениях.

В случае, если изменены следующие категорий персональных данных работника:

* фамилия;
* имя;
* отчество;
* паспортные данные;
* дата рождения;
* адрес проживания;
* адрес постоянной регистрации;
* гражданство;

с работником заключается дополнительно соглашение к трудовому договору с указанием изменившихся персональных данных.

* 1. Уничтожение персональных данных осуществляется в срок, не превышающий 30 рабочих дней с момента достижения цели обработки персональных данных, если иное не предусмотрено федеральными законами Российской Федерации.
	2. Уничтожение персональных данных осуществляется в срок, не превышающий 30 рабочих дней с момента отзыва согласия субъекта персональных данных на обработку персональных данных. Форма отзыва согласия приведена в приложении №5 к настоящему положению. Лицам, ответственным за администрирование официальных информационных ресурсов Общества в информационно-телекоммуникационных сетях, необходимо обеспечить публикацию формы отзыва согласия на этих информационных ресурсах.
	3. Уничтожение персональных данных осуществляется в срок, не превышающий 7 рабочих дней с момента представления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки.
	4. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его законного представителя и невозможности обеспечить правомерную обработку персональных данных уничтожение персональных данных осуществляется в срок, не превышающий 10 рабочих дней с момента выявления неправомерной обработки персональных данных. Решение о неправомерности обработки персональных данных и необходимости уничтожения персональных данных принимает ответственный за организацию обработки персональных данных, который доводит соответствующую информацию до руководства Общества. Общество уведомляет субъекта персональных данных или его законного представителя об уничтожении персональных данных.
	5. Уничтожение персональных данных осуществляет временная комиссия в составе работников структурного подразделения, обрабатывавшего подлежащие уничтожению персональные данные субъекта, под контролем руководителя этого структурного подразделения.
	6. Способ уничтожения материальных носителей персональных данных определяется временной комиссией. Допускается применение следующих способов:
1. сжигание;
2. шредирование (измельчение);
3. передача на специализированные полигоны (свалки);
4. химическая обработка.

При этом составляется акт, подписываемый председателем временной комиссии, проводившей уничтожение материальных носителей персональных данных. Форма акта приведена в приложении №6 к настоящему Положению.

При необходимости уничтожения большого количества материальных носителей или применения специальных способов уничтожения допустимо привлечение специализированных организаций. В этом случае временная комиссия Общества должна присутствовать при уничтожении материальных носителей персональных данных. При этом к акту уничтожения необходимо приложить накладную на передачу материальных носителей персональных данных, подлежащих уничтожению, в специализированную организацию.

* 1. Уничтожение полей баз данных Общества, содержащих персональные данные субъекта, выполняется в случаях, установленных в пункте 4.16 по заявке руководителя структурного подразделения, обрабатывавшего персональные данные субъекта и установившего необходимость их уничтожения.
	2. Уничтожение осуществляет временная комиссия, в состав которой входят лица, ответственные за техническое обслуживание автоматизированных систем, которым принадлежат базы данных.
	3. Уничтожение достигается путем затирания информации на носителях информации (в том числе и резервных копиях). При этом составляется акт, утверждаемый лицом, ответственным за техническое обслуживание информационных систем, которым принадлежат базы данных.
	4. Уничтожение архивов электронных документов и протоколов электронного взаимодействия может не производиться, если ведение и сохранность их в течение определенного срока предусмотрены соответствующими нормативными и (или) договорными документами.
	5. При отсутствии технической возможности осуществить уничтожение персональных данных, содержащихся в базах данных, допустимо проведение обезличивания путем перезаписи полей баз данных. Перезапись должна быть осуществлена таким образом, чтобы дальнейшая идентификация субъекта персональных данных была не возможна.
	6. Контроль выполнения процедур уничтожения персональных данных осуществляет ответственный за организацию обработки персональных данных.
	7. Обработка биометрических персональных данных (фотография, используемая для идентификации), в соответствии со статьей 11 Федерального закона № 152-ФЗ, допускается при наличии согласия субъекта. Форма согласия определена в приложении №1 к настоящему Положению.
	8. Решение, порождающее юридические последствия в отношении субъекта персональных данных или иным образом затрагивающее его права и законные интересы, может быть принято на основании исключительно автоматизированной обработки его персональных данных только при наличии согласия в письменной форме субъекта персональных данных[[2]](#footnote-2).
	9. Работники должны быть ознакомлены под подпись с настоящим Положением и другими документами Общества, устанавливающими порядок обработки персональных данных субъектов, а также права и обязанности в этой области.

# ПРАВИЛА РАБОТЫ С ОБЕЗЛИЧЕННЫМИ ДАННЫМИ

* 1. Порядок обезличивания включает в себя замену идентифицирующей информации о субъекте (например: фамилию, имя и отчество) на произвольный код (далее – идентификатор).
	2. Обезличивание должно проводиться таким образом, чтобы определить принадлежность персональных данных конкретному субъекту персональных данных было невозможно без использования дополнительной информации.
	3. В случае, если обезличенные персональные данные используются в статистических или иных исследовательских целях, сроки обработки и хранения персональных данных устанавливаются руководством Общества исходя из служебной необходимости, и получение согласия субъекта на обработку его персональных данных не требуется[[3]](#footnote-3).
	4. Если обезличенные персональные данные используются в целях продвижения товаров, работ, услуг на рынке, Общество обязано получить согласие субъекта персональных данных на подобную обработку.
	5. Методы и способы защиты информации от несанкционированного доступа для обеспечения безопасности обезличенных персональных данных в информационных системах и целесообразность их применения определяются ответственным за защиту информации в Обществе индивидуально для каждой информационной системы персональных данных.

# ПЕРЕДАЧА ПЕРСОНАЛЬНЫХ ДАННЫХ ТРЕТЬИМ ЛИЦАМ

* 1. При обработке персональных данных субъекта должны соблюдаться следующие требования:
1. Не сообщать персональные данные субъекта третьей стороне без письменного согласия субъекта в форме, определенной настоящим Положением;
2. Предупреждать лиц (путем инструктажей либо путем включения соответствующих норм в договор), получающих персональные данные субъекта, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные субъекта, обязаны соблюдать режим конфиденциальности в отношении этих данных.
	1. При необходимости передачи персональных данных работников Общества и членов их семей профсоюзной организации, порядок осуществления такой передачи должен удовлетворять следующим правилам:
* передача осуществляется только по письменному запросу профсоюзной организации и с разрешения руководителя Общества;
* передача персональных данных осуществляется либо в бумажном виде с описью и фиксацией в соответствующем реестре исходящей корреспонденции, либо в электронном виде путем передачи защищенного (зашифрованного с применением сертифицированных криптографических средств) сообщения[[4]](#footnote-4).

Для упрощения порядка обмена персональными данными между Обществом и профсоюзной организацией допустимо однократно заключить соглашение об информационном обмене. В соглашении определить порядок запроса и получения персональных данных, категории и состав передаваемых персональных данных, лиц, уполномоченных на передачу и получение персональных данных.

* 1. При необходимости трансграничной передачи персональных данных на территорию иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных, Общество запрашивает согласие субъекта в письменной форме. Форма согласия определена в приложении №3 к настоящему Положению.
	2. Не допускается применение информационно-телекоммуникационных сетей Общества для сбора персональных данных работников Общества и членов их семей сторонними организациями.

# ПРАВА СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

* 1. В целях обеспечения своих интересов субъекты имеют право:
1. получать полную информацию о своих персональных данных и обработке этих данных (в том числе автоматизированной);
2. получить разъяснения о юридических последствиях отказа предоставить персональные данные свои или членов своей семьи Обществу (форма разъяснения приведена в приложении №4 к настоящему Положению);
3. осуществлять свободный бесплатный доступ к своим персональным данным, включая право получать копии любой записи, содержащей персональные данные субъекта, за исключением случаев, предусмотренных Федеральным законом № 152-ФЗ;
4. требовать исключения или исправления неверных, или неполных персональных данных, а также данных, обработанных с нарушением Федерального закона № 152-ФЗ. Субъект, при отказе Общества исключить или исправить персональные данные субъекта, имеет право заявлять в письменной форме о своем несогласии, обосновав соответствующим образом такое несогласие. Персональные данные оценочного характера субъект имеет право дополнить заявлением, выражающим его собственную точку зрения;
5. требовать от Общества уведомления всех лиц, которым ранее были сообщены неверные или неполные персональные данные субъекта, обо всех произведенных в них изменениях или исключениях из них[[5]](#footnote-5);
6. обжаловать в суд любые неправомерные действия или бездействие Общества при обработке и защите персональных данных субъекта.
	1. Учет запросов граждан на предоставление информации об обработке их персональных данных в Обществе выполняет отдел кадров путем ведения советующего журнала. Форма журнала приведена в приложении №7 к настоящему положению. Ответственный за организацию обработки персональных данных контролирует полноту и своевременность исполнения указанных запросов граждан.

# ПОРЯДОК ДЕЙСТВИЙ ПРИ ПОЛУЧЕНИИ ЗАПРОСОВ НАДЗОРНЫХ ОРГАНОВ

* 1. В соответствии с частью 4 статьи 20 Федерального закона № 152-ФЗ Общество сообщает в уполномоченный орган по защите прав субъектов персональных данных по его запросу информацию, необходимую для осуществления деятельности указанного органа, в течение тридцати дней с даты получения такого запроса.
	2. Сбор сведений для составления мотивированного ответа на запрос надзорных органов осуществляет ответственный за организацию обработки персональных данных при необходимости с привлечением работников Общества.
	3. В течение установленного законодательством срока ответственный за организацию обработки персональных данных подготавливает и направляет в уполномоченный орган мотивированный ответ и другие необходимые документы.

# ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ СУБЪЕКТОВ

* 1. Защиту персональных данных субъектов от неправомерного их использования или утраты Общество обеспечивает за счет собственных средств в порядке, установленном законодательством Российской Федерации.

При обработке персональных данных должны быть приняты необходимые организационные и технические меры по обеспечению их конфиденциальности, доступности, целостности.

Технические меры защиты персональных данных при их обработке техническими средствами устанавливаются в соответствии с:

1. РД ФСТЭК России - "Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных". Утверждены приказом ФСТЭК России № 21 от 18 февраля 2013 года;
2. специальными требованиями и рекомендациями по технической защите конфиденциальной информации (СТР-К), утвержденными приказом Гостехкомиссии России от 30 августа 2002 года № 282;
3. внутренними документами Общества, действующими в сфере обеспечения информационной безопасности;
4. иными руководящими документами.
	1. Защита персональных данных предусматривает ограничение к ним доступа.
	2. Руководитель структурного подразделения Общества, осуществляющего обработку персональных данных:
5. несет ответственность за организацию защиты персональных данных в подчиненном структурном подразделении;
6. закрепляет за работниками, уполномоченными обрабатывать персональные данные, конкретные материальные носители, на которых допускается хранение персональных данных в случае, если такие носители необходимы для выполнения возложенных на работников функций;
7. организует изучение подчинёнными работниками, в чьи обязанности входит обработка персональных данных, нормативных правовых актов по защите персональных данных и требует их неукоснительного исполнения;
8. обеспечивает режим конфиденциальности в отношении персональных данных, обрабатываемых в структурном подразделении;
9. организует контроль доступа к персональным данным в соответствии с функциональными обязанностями работников подразделения.
	1. Работники, допущенные к персональным данным, дают письменное обязательство о неразглашении таких данных. Сбор обязательств выполняет отдел кадров Общества при назначении работника на должность, предусматривающую обработку персональных данных. Форма обязательства приведена в приложении №3 к настоящему Положению.
	2. При выборе организационных и технических мер защиты персональных данных, определении актуальных угроз обязательно необходимо, помимо прочего, учитывать размер возможного ущерба субъектам персональных данных в случае нарушения конфиденциальности, доступности, целостности их персональных данных и персональных данных членов их семей. Оценку вреда субъектам персональных данных в случае нарушения порядка обработки их персональных данных или их целостности должна выполнять ПДК ЗИ. Пересмотр оценки вреда необходимо выполнять при каждом изменении перечня целей обработки персональных данных, условий их обработки, состава обрабатываемых персональных данных.
	3. ПДК ЗИ обязана не менее одного раза в год проводить проверку соответствия установленного в Обществе порядка обработки персональных данных требованиям действующего законодательства Российской Федерации, а также соответствия выбранных мер защиты персональных данных требованиям законодателя и регуляторов. Результаты проверки и рекомендации по устранению выявленных нарушений оформляются в виде акта и направляются на утверждение руководителю Общества.

# ОБЯЗАННОСТИ ЛИЦ, ДОПУЩЕННЫХ К ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

* 1. Лица, допущенные к работе с персональными данными, обязаны:
1. знать законодательство Российской Федерации в области обработки и защиты персональных данных, нормативные документы Общества по защите персональных данных;
2. сохранять конфиденциальность персональных данных;
3. обеспечивать сохранность закрепленных за ними носителей персональных данных;
4. контролировать срок истечения действия согласий на обработку персональных данных и, при необходимости дальнейшей обработки персональных данных, обеспечивать своевременное получение новых согласий или прекращение обработки персональных данных;
5. докладывать своему непосредственному руководителю отдела (структурного подразделения) обо всех фактах и попытках несанкционированного доступа к персональным данным и других нарушениях.

# ОТВЕТСТВЕННОСТЬ РАБОТНИКА ЗА НАРУШЕНИЕ НОРМ, РЕГУЛИРУЮЩИХ ОБРАБОТКУ И ЗАЩИТУ ПЕРСОНАЛЬНЫХ ДАННЫХ СУБЪЕКТОВ

* 1. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, привлекаются к материальной, административной, уголовной и гражданско-правовой ответственности на основании судебного решения, а также к дисциплинарной ответственности в рамках действующего законодательства Российской Федерации.

# НОРМАТИВНЫЕ ССЫЛКИ

* 1. Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных от 28.01.1981 с поправками, одобренными Комитетом министров Совета Европы 15.06.1999, ратифицированная Федеральным законом РФ от 19.12.2005 №160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных» в рамках, определяемых данным Федеральным законом, заявлений.
	2. Конституция РФ;
	3. Федеральный закон РФ от 27.07.2006 № 152-ФЗ «О персональных данных»;
	4. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
	5. Постановление Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
	6. Постановление Правительства РФ от 06.07.2008 № 512 «Об утверждении Требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;
	7. Состав и содержание 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 РФ требований к защите персональных данных для каждого из уровней защищенности, утвержденные приказом ФСБ России от 10.07.2014 №378;
	8. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утверждена ФСТЭК России 14.02.2008 г.;
	9. Специальные требования и рекомендации по технической защите конфиденциальной информации одобренные решением коллегии Гостехкомиссии России от 02.03.2001 № 7.2;
	10. Требования о защите информации, содержащейся в информационных системах общего пользования, утверждённые совместным приказом ФСБ России и ФСТЭК России от 31.08.2010 № 416/489;
	11. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утверждённые приказом ФСТЭК России от 18.02.2013 № 21;

# Приложение №1

к положению о порядке обработки

персональных данных

Руководителю
ООО «Ромашка»

**СОГЛАСИЕ
на обработку персональных данных субъекта, в том числе биометрических персональных данных**

Я, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, \_\_\_\_\_ г.р., проживающий (-ая) по адресу \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, в соответствии с Федеральным законом Российской Федерации от 27 июля 2006 года № 152-ФЗ "О персональных данных", даю согласие ООО «Ромашка», расположенному по адресу: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, на обработку моих персональных данных, а именно:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | * *ФИО;*
 |  | * *Адреса регистрации и проживания;*
 |  | * *Образование;*
 |
|  | * *Дата рождения;*
 |  | * *Паспортные данные;*
 |  | * *Доходы;*
 |
|  | * *Место рождения;*
 |  | * *Семейное положение;*
 |  | * *Профессия;*
 |
|  | * *Фотография;*
 |  | * *Сведения о состоянии здоровья;*
 |  | * *Контактные данные*
 |
|  | * *Сведения о трудоспособности;*
 |  | * *Сведения о трудовой деятельности;*
 |  | * *Сведения о воинском учете;*
 |
|  | * *Сведения о составе семьи*
 |  | * *Социальное положение*
 |  | * *Имущественное положение*
 |
| (нужное отметить) |
|  | и другие: |
|   |
|   |
| (перечислить дополнительные категории персональных данных) |
| В целях |  |
|
|   |
|   |

Перечень допустимых действий, осуществляемых с персональными данными: *сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, обезличивание, блокирование, уничтожение;*

(ненужное зачеркнуть)

ООО «Ромашка» может осуществлять автоматизированную, смешанную, неавтоматизированную обработку персональных данных с применением ЭВМ, с передачей по внутренней сети и с передачей по сети интернет (с условием применения необходим мер защиты информации).

Согласие вступает в силу со дня его подписания и действует в течение \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. Действие настоящего согласия прекращается досрочно в случае принятия оператором решения о прекращении обработки персональных данных и/или уничтожения документов, содержащих персональные данные.
 Согласие может быть отозвано мною в любое время на основании моего письменного заявления.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| "\_\_\_" \_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ года |  |  |  |  |
|  |  | (подпись) |  | (инициалы, фамилия) |

Руководителю
ООО «Ромашка»

**СОГЛАСИЕ
на обработку персональных данных ребёнка работника**

Я, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, \_\_\_\_\_ г.р., проживающий (-ая) по адресу \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, в соответствии с Федеральным законом Российской Федерации от 27 июля 2006 года № 152-ФЗ "О персональных данных", даю согласие ООО «Ромашка», расположенному по адресу: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, на обработку персональных данных моего ребёнка \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, законным представителем которого я являюсь, а именно:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | * *ФИО;*
 |  | * *Адрес*
 |  | * *Образование*
 |
|  | * *Дата рождения;*
 |  | * *Пол*
 |  | * *Данные свидетельства о рождении*
 |
|  | * *Место рождения;*
 |  |  |  |
| (нужное отметить) |
| и другие:  |
|   |
|   |
| (перечислить дополнительные категории персональных данных) |

В целях: выплаты пособия на ребёнка; получения налогового вычета по НДФЛ; предоставления бухгалтерской и статистической отчётности; обеспечения соблюдения законов и иных правовых актов, проведение творческих, спортивных и иных мероприятий.

Даю свое согласие ООО «Ромашка» на передачу (включая предоставление, доступ) с использованием средств автоматизации и/или без использования таких средств вышеуказанных персональных данных моего ребёнка третьему лицу, а именно: в налоговые инспекции, органы социального страхования с целью соблюдения законов и иных правовых актов.

|  |
| --- |
| а также: |
|   |
|   |
| (указать третьих лиц при необходимости) |

Перечень допустимых действий, осуществляемых с персональными данными: *сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, обезличивание, блокирование, уничтожение;*

(ненужное зачеркнуть)

ООО «Ромашка» может осуществлять автоматизированную, смешанную, неавтоматизированную обработку персональных данных с применением ЭВМ, с передачей по внутренней сети и с передачей по сети интернет (с условием применения необходим мер защиты информации).

Согласие вступает в силу со дня его подписания и действует в течение исполнения мной трудовых обязанностей (срока действия трудового контракта), а также в течении 5 лет после прекращения действия трудового контракта.

Действие настоящего согласия прекращается досрочно в случае принятия оператором решения о прекращении обработки персональных данных и/или уничтожения документов, содержащих персональные данные.

Согласие может быть отозвано мною в любое время на основании моего письменного заявления.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| "\_\_\_" \_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ года |  |  |  |  |

Руководителю
ООО «Ромашка»

**СОГЛАСИЕ
субъекта на передачу его персональных данных третьей стороне**

Я, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, \_\_\_\_\_ г.р., проживающий (-ая) по адресу \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, в соответствии с Федеральным законом Российской Федерации от 27 июля 2006 года № 152-ФЗ "О персональных данных" даю согласие ООО «Ромашка»расположенному по адресу: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, на передачу моих персональных данных, а именно:

|  |
| --- |
|  |
|  | * *ФИО*
 |  | * *Адрес*
 |  | * *Образование*
 |
|  | * *Дата рождения*
 |  | * *Паспортные данные*
 |  | * *Доходы*
 |
|  | * *Место рождения*
 |  | * *Семейное положение*
 |  | * *Профессия*
 |
|  | * *Фотография*
 |  | * *Сведения о здоровье*
 |  | * *Сведения о трудоспособности*
 |
| (нужное отметить) |
|  | и другие: |
|  |   |
|  |   |  |  |  |  |
| (перечислить дополнительные категории персональных данных) |
|  |
| Для обработки в целях |  |
|  |
|  |
|   |
| (указать цели обработки) |
|  |
| Следующим лицам |  |
|  |
|  |
|   |
|   |
| (указать Ф.И.О., адрес физического лица или наименование и адрес организации, которым сообщаются данные) |
|  |

Перечень допустимых действий, осуществляемых с персональными данными: *сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, обезличивание, блокирование, уничтожение;*

|  |
| --- |
|  |

(ненужное зачеркнуть)

ООО «Ромашка» может осуществлять автоматизированную, смешанную, неавтоматизированную обработку персональных данных с применением ЭВМ, с передачей по внутренней сети и с передачей по сети интернет (с условием применения необходим мер защиты информации).

Согласие вступает в силу со дня его подписания и действует в течение \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. Действие настоящего согласия прекращается досрочно в случае принятия оператором решения о прекращении обработки персональных данных и/или уничтожения документов, содержащих персональные данные.

Согласие может быть отозвано мною в любое время на основании моего письменного заявления.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| "\_\_\_" \_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ года |  |  |  |  |
|  |  | (подпись) |  | (инициалы, фамилия) |

Руководителю
ООО «Ромашка»

**СОГЛАСИЕ
субъекта на трансграничную передачу персональных данных**

Я, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, \_\_\_\_\_\_\_\_г.р., проживающий (-ая) по адресу \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, в соответствии с Федеральным законом Российской Федерации от 27 июля 2006 года № 152-ФЗ "О персональных данных" даю согласие ООО «Ромашка», расположенному по адресу: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, на трансграничную передачу моих персональных данных:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | * *ФИО*
 |  | * *Адрес*
 |  | * *Образование*
 |
|  | * *Дата рождения*
 |  | * *Паспортные данные*
 |  | * *Доходы*
 |
|  | * *Место рождения*
 |  | * *Семейное положение*
 |  | * *Профессия*
 |
| (ненужное зачеркнуть) |
|  | и другие: |
|  |   |
|  |   |  |  |  |  |
| (перечислить дополнительные категории персональных данных) |

на территорию иностранного государства, не обеспечивающего адекватной защиты прав субъектов персональных данных:

|  |
| --- |
|  |
|   |
|   |
| (указать страну адресат, подразделение (филиал) организации или наименование и адрес сторонней организации , которым сообщаются данные) |
|  |
| В целях |  |
|  |
|   |
| (указать цели обработки) |
|  |

Перечень допустимых действий, осуществляемых с персональными данными: *сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, обезличивание, блокирование, уничтожение;*

|  |
| --- |
|  |

(ненужное зачеркнуть)

ООО «Ромашка» может осуществлять автоматизированную, смешанную, неавтоматизированную обработку персональных данных с применением ЭВМ, с передачей по внутренней сети и с передачей по сети интернет (с условием применения необходим мер защиты информации).

Согласие вступает в силу со дня его подписания и действует в течение \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. Действие настоящего согласия прекращается досрочно в случае принятия оператором решения о прекращении обработки персональных данных и/или уничтожения документов, содержащих персональные данные.

Согласие может быть отозвано мною в любое время на основании моего письменного заявления.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| "\_\_\_" \_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ года |  |  |  |  |
|  |  | (подпись) |  | (инициалы, фамилия) |

# Приложение №2

к положению о порядке обработки

персональных данных

Руководителю
ООО «Ромашка»

**СОГЛАСИЕ
субъекта на получение его персональных данных у третьей стороны**

Я, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, \_\_\_\_\_ г.р., проживающий (-ая) по адресу \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, в соответствии с Федеральным законом Российской Федерации от 27 июля 2006 года № 152-ФЗ "О персональных данных", даю согласие ООО «Ромашка», расположенному по адресу: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, на получение моих персональных данных у третьей стороны, а именно:

|  |
| --- |
|   |
|   |
| (указать третьих лиц) |
|  | * *ФИО*
 |  | * *Адрес*
 |  | * *Образование*
 |
|  | * *Дата рождения*
 |  | * *Паспортные данные*
 |  | * *Доходы*
 |
|  | * *Место рождения*
 |  | * *Семейное положение*
 |  | * *Профессия*
 |
|  | (нужное отметить) |
|  | и другие: |
|   |
|   |
| (перечислить дополнительные категории персональных данных) |
|  |
| В целях |
|   |
| (указать цели обработки) |
|  |
| Перечень допустимых действий, осуществляемых с персональными данными: *сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, обезличивание, блокирование, уничтожение;* |

(ненужное зачеркнуть)

ООО «Ромашка» может осуществлять автоматизированную, смешанную, неавтоматизированную обработку персональных данных с применением ЭВМ, с передачей по внутренней сети и с передачей по сети интернет (с условием применения необходим мер защиты информации).

Согласие вступает в силу со дня его подписания и действует в течение \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. Действие настоящего согласия прекращается досрочно в случае принятия оператором решения о прекращении обработки персональных данных и/или уничтожения документов, содержащих персональные данные.

Согласие может быть отозвано мною в любое время на основании моего письменного заявления.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| "\_\_\_" \_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ года |  |  |  |  |
|  |  | (подпись) |  | (инициалы, фамилия) |

# Приложение №3

к положению о порядке обработки

персональных данных

**ТИПОВОЕ ОБЯЗАТЕЛЬСТВО
работника ООО «Ромашка» о неразглашении персональных данных субъектов персональных данных**Я, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, \_\_\_\_\_ г.р., проживающий (-ая) по адресу \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, ,  работая в должности\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
в ООО «Ромашка» (далее – Общество), в период настоящих трудовых отношений и в течение 5 лет после их окончания, в соответствии с Федеральным законом Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных», обязуюсь:

|  |
| --- |
|  |

1) не раскрывать третьим лицам и не распространять персональные данные субъектов Общества, полученные при исполнении мной трудовых обязанностей;

2) при работе с персональными данными соблюдать требования, описанные в «Правилах обработки персональных данных субъектов Общества;

3) выполнять относящиеся ко мне требования локальных нормативных актов, касающихся обработки персональных данных;

4) в случае попытки посторонних лиц получить от меня персональные данные субъектов персональных данных Общества, сведения о порядке обработки и защиты персональных данных немедленно уведомить об этом руководителя своего структурного подразделения;

5) в случае расторжения со мною трудового договора или контракта, прекратить обработку персональных данных, ставших известными мне в связи с исполнением должностных обязанностей, и передать все носители персональных данных субъектов Общества (документы, накопители данных в электронном виде, кино и фотонегативы и позитивы, и пр.) ответственному за обработку персональных данных Общества.

Я понимаю, что разглашение персональных данных субъектов Общества, может нанести ущерб субъектам персональных данных.

Я предупрежден(а) о том, что в случае разглашения или утраты мною сведений, относящихся к персональным данным субъектов Общества, я несу ответственность в соответствии со статьей 90 Трудового Кодекса РФ и могу быть привлечён к дисциплинарной, материальной, гражданско-правовой, административной и уголовной ответственности в соответствие с действующим законодательством Российской Федерации.

Настоящим подтверждаю, что с «Положением о порядке обработки персональных данных субъектов Общества» ознакомлен.

"\_\_\_\_" \_\_\_\_\_\_\_\_\_\_\_ 201\_ года \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# Приложение №4

к положению о порядке обработки

персональных данных

**ТИПОВАЯ ФОРМА
разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные**

В соответствии с принципами обработки персональных данных, установленными Федеральным законом Российской Федерации от 27 июля 2006 года № 152-ФЗ "О персональных данных", при обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, и актуальность по отношению к заявленным целям обработки персональных данных.

Кроме того, оператор должен принимать необходимые меры по уточнению неполных или неточных персональных данных.

В случае, если субъект персональных данных отказывается предоставить свои персональные данные, либо представленные персональные данные являются неточными и (или) неполными по отношению к заявленным целям обработки персональных данных, ООО «Ромашка» (далее – Общество) оставляет за собой право отказать в предоставлении своих услуг, в продолжении трудовых или договорных отношений субъекту персональных данных.

Если Общество выявит факт умышленного представления субъектом неверных персональных данных, то Общество может потребовать с субъекта возмещения соответствующих затрат.

Ответственный за организацию \_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_/

обработки персональных данных

в ООО «Ромашка»

# Приложение №5

к положению о порядке обработки

персональных данных

Руководителю

ООО «Ромашка»

|  |  |
| --- | --- |
|  |  |
|  | Ф.И.О. субъекта персональных данных, год рождения |
|  |  |
|  | Адрес регистрации субъекта |
|  |  |
|  | Адрес проживания |
|  |  |
|  | Контактные сведения |

**ЗАЯВЛЕНИЕ**

|  |
| --- |
|   Прошу Вас прекратить обработку моих персональных данных в связи с |
|   |
|   |
| (указать причину) |
| "\_\_\_"\_\_\_\_\_\_\_\_\_\_\_\_ 201\_\_ года |  \_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  | (подпись) (расшифровка подписи)  |

# Приложение №6

к положению о порядке обработки

персональных данных

**А К Т № \_\_\_\_\_
уничтожения документов ООО «Ромашка», содержащих персональные данные субъекта**

|  |  |
| --- | --- |
| Состав комиссии:  |  |
| Председатель комиссии: | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Члены комиссии: | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

Комиссия произвела отбор к уничтожению следующих документов, содержащих персональные данные субъекта персональных данных:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| №п/п | Наименованиедокумента | Регистрационный номер документа | Датарегистрации | Номер экз. | Количество листов документа /приложения |
| 1 | 2 | 3 | 4 | 5 | 6 |
|  |  |  |  |  |  |

Причина уничтожения:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| □ | достижение целей обработки персональных данных | □ | решение субъекта персональных данных | □ | недостоверные персональные данные |
| Всего подлежит уничтожению \_\_\_\_\_\_ (\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_)  |
|  | (цифрами) | (прописью) |
| наименований документов. |
| Документы уничтожены с помощью \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|   |
| (указать способ уничтожения) |
| Председатель комиссии: | \_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Члены комиссии: | \_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  | \_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  | \_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

**А К Т № \_\_\_\_\_
уничтожения полей баз данных ООО «Ромашка», содержащих персональные данные субъекта**

|  |  |
| --- | --- |
| Состав комиссии:  |  |
| Председатель комиссии: | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Члены комиссии: | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

Комиссия произвела отбор к уничтожению следующих полей баз данных, содержащих персональные данные субъекта персональных данных:

|  |  |  |  |
| --- | --- | --- | --- |
| №п/п | Наименование базы данных | Идентификационный номер поля данных | Наименование полей данных |
| 1 | 2 | 3 | 4 |
|  |  |  |  |

Причина уничтожения:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| □ | достижение целей обработки персональных данных | □ | решение субъекта персональных данных | □ | недостоверные персональные данные |
| Всего подлежит уничтожению \_\_\_\_\_\_ (\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_)  |
|  | (цифрами) | (прописью) |
| наименований полей базы данных. |
| Поля баз данных уничтожены путем затирания информации на носителях информации (в том числе и резервных копиях).  |
| Председатель комиссии: | \_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Члены комиссии: | \_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  | \_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  | \_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

# Приложение №7

к положению о порядке обработки

персональных данных

|  |
| --- |
| ООО «Ромашка» |

**ЖУРНАЛ
регистрации письменных запросов граждан
на доступ к своим персональным данным**

|  |  |
| --- | --- |
| Журнал начат "\_\_\_\_" \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ года | Журнал завершен "\_\_\_\_" \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ года  |
| Ответственный за организацию обработкиПерсональных данных | Ответственный за организацию обработкиПерсональных данных |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/ |

На \_\_\_\_\_ листах

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| №п/п | Вх. № письма | Дата получения запроса | Ф.И.О. гражданина | Отношения субъекта ПДн с оператором ПДн | Отметка о предоставлении доступа к ПДн(отказе в доступе) | Исх. номер и дата письма с ответом на запрос | Ф.И.О., должность, подпись работника, выдавшего ответ |  |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

# Приложение №8

к положению о порядке обработки

персональных данных

**ИНСТРУКЦИЯ
по осуществлению внутреннего контроля выполнения требований по защите персональных данных в ООО «Ромашка»**

Настоящая инструкция определяет порядок организации и осуществления контроля выполнения требований по защите персональных данных в структурных подразделениях ООО «Ромашка» (далее – Общество).

Требования инструкции обязательны для исполнения всеми должностными лицами Общества, осуществляющими контроль состояния защиты персональных данных.

1. Общие положения

Контроль выполнения требований по защите персональных данных в структурных подразделениях Общества осуществляется с целью определения наличия несоответствий между требуемым уровнем защиты персональных данных и его фактическим состоянием, а также выработать меры по их устранению и недопущению в дальнейшем.

Контроль осуществляет ответственный за организацию обработки персональных данных Общества (далее – Ответственный). Для участия в проведении контроля по решению Ответственного может привлекаться постоянно действующая комиссия по защите информации. В таких случаях контроль носит комплексный характер.

Контроль проводится в форме плановых и внеплановых проверок. Внеплановые проверки могут быть контрольными и по частным вопросам.

Контрольные проверки проводятся для установления полноты выполнения рекомендаций плановых проверок.

Проверки по частным вопросам охватывают отдельные направления по защите персональных данных и могут проводиться в случаях, когда стали известны факты несанкционированного доступа, утечки либо утраты персональных данных субъектов Общества или нарушения требований по защите персональных данных.

Сроки проведения контрольных проверок доводятся руководителям проверяемых структурных подразделений не позднее, чем за 24 часа до начала проверки.
 Проверки по частным вопросам могут проводиться без уведомления руководителей проверяемых подразделений.
 Периодичность и сроки проведения плановых проверок подразделений Общества устанавливаются графиком проверок на календарный год. План утверждает руководитель Общества. Сроки проведения плановых проверок доводятся руководителям проверяемых подразделений не позднее, чем за 10 суток до начала проверки.

2. Порядок подготовки к проверке

Проверка проводится на основании приказа руководителя Общества. Осуществляет проверку постоянно действующая комиссия по защите информации.

Ответственный за организацию обработки персональных данных Общества должен входить в состав указанной комиссии. Проект приказа о проверке подготавливает Ответственный.

Проверяющие лица обязаны получить у руководителей проверяемых структурных подразделений информацию об условиях обработки персональных данных, необходимую для достижения целей проверки. Перед началом проверки они должны изучить материалы предыдущих проверок данного структурного подразделения.

3. Порядок проведения проверки

По прибытию в подразделение для проведения проверки председатель комиссии прибывает к руководителю проверяемого подразделения Общества, представляется ему и представляет других прибывших на проверку лиц.

Руководитель проверяемого структурного подразделения обязан оказывать содействие комиссии и, в случае необходимости, определяет должностное лицо, ответственное за сопровождение проверки.

На период проведения контрольных мероприятий обработку персональных данных необходимо по возможности прекращать. Допуск проверяющих лиц к конкретным информационным ресурсам, защищаемым сведениям и техническим средствам должен исключать ознакомление проверяющих лиц с конкретными персональными данными.

Общий порядок проведения проверки включает следующее:

1) получение документов о распределении обязанностей по обработке и защите персональных данных, выявление ответственных за обработку и защиту персональных данных и установление факта ознакомления работников проверяемого структурного подразделения со своей ответственностью;
 2) получение при содействии работников проверяемого структурного подразделения документов, касающихся обработки и защиты персональных данных в данном структурном подразделении;
 3) анализ полученной документации;
 4) непосредственная проверка выполнения установленного порядка обработки и защиты персональных данных и требований законодательства Российской Федерации в области защиты персональных данных.
 При этом согласовываются конкретные вопросы по объему, содержанию, срокам проведения проверки, а также каких должностных лиц подразделения необходимо привлечь к проверке и какие объекты следует посетить.
 В ходе осуществления контроля выполнения требований по защите персональных данных в подразделении Общества рассматриваются в частности следующие показатели:
 1) в части общей организации работ по защите персональных данных:
 а) соответствие информации, указанной в уведомлении об обработке персональных данных, реальному положению дел;
 б) наличие нормативных документов по защите персональных данных;
 в) знание нормативных документов работниками, имеющими доступ к персональным данным;
 г) полнота и правильность выполнения требований нормативных документов работниками, имеющими доступ к персональным данным;
 д) наличие документов, определяющих состав работников, ответственных за организацию защиты персональных данных в подразделении, соответствие этих документов реальному штатному составу подразделения, а также подтверждение факта ознакомления ответственных работников с данными документами;
 е) уровень подготовки работников, ответственных за организацию защиты персональных данных в подразделении;
 ж) наличие согласий на обработку персональных данных субъектов персональных данных. Соответствие объёма персональных данных и сроков обработки целям обработки персональных данных.
 2) в части защиты персональных данных в информационных системах персональных данных (далее - ИСПДн):
 а) соответствие средств вычислительной техники ИСПДн показателям, указанным в документации на ИСПДн;
 б) структура и состав локальных вычислительных сетей, организация разграничения доступа пользователей к сетевым информационным ресурсам, порядок защиты охраняемых сведений при передаче (обмене) персональных данных в сети передачи данных;
 в) соблюдение установленного порядка использования средств вычислительной техники ИСПДн;
 г) наличие и эффективность применения средств и методов защиты персональных данных, обрабатываемых на средствах вычислительной техники;

д) соблюдение требований, предъявляемых к паролям на информационные ресурсы;

е) соблюдение требований и правил антивирусной защиты средств вычислительной техники;

ж) контроль журналов учета носителей персональных данных. Сверка основного журнала с дублирующим (если требуется ведение дублирующего учета носителей);

з) тестирование реализации правил фильтрации межсетевого экрана, процесса регистрации, процесса идентификации и аутентификации запросов, процесса идентификации и аутентификации администратора межсетевого экрана, процесса регистрации действий администратора межсетевого экрана, процесса контроля за целостностью программной и информационной части, процедуры восстановления настроек межсетевого экрана.

3) в части защиты информационных ресурсов и помещений:

а) правильность отнесения обрабатываемой информации к персональным данным;

б) правильность классификации информационной системы;

в) закрепление гражданско-правовой ответственности в сфере информационной безопасности и соблюдения режима конфиденциальности персональных данных в правилах внутреннего трудового распорядка, положениях о подразделениях Общества, должностных инструкциях работников и трудовых договорах;

г) порядок передачи персональных данных органам государственной власти, местного самоуправления и сторонним организациям (контрагентам);

д) действенность принимаемых мер по защите охраняемых сведений в ходе подготовки материалов к открытому опубликованию и при изготовлении рекламной продукции;

е) состояние конфиденциального делопроизводства, соблюдение установленного порядка подготовки, учета, использования, хранения и уничтожения документов, содержащих персональные данные;

ж) выполнение требований по правильному оборудованию защищаемых помещений и предотвращению утечки охраняемых сведений при проведении мероприятий конфиденциального характера;

з) соответствие защищаемых помещений их техническим паспортам.

Более подробно вопросы, подлежащие проверке, могут раскрываться в отдельных документах (методических рекомендациях, технологических картах, памятках и т.п.).

Во время проведения проверки, выявленные нарушения требований по обработке и защите персональных данных должны быть по возможности устранены. Проверяющие лица могут дать рекомендации по устранению на месте отмечаемых нарушений и недостатков.

Недостатки, которые не могут быть устранены на месте, включаются в итоговый документ по результатам проверки.

4. Оформление результатов проверки

Результаты проверки оформляются актом, представляемым на утверждение руководителю Общества.

Акт составляется в двух экземплярах и подписывается членами комиссии. Один экземпляр хранится у Ответственного. Второй экземпляр хранится в Обществе в установленном порядке. Копия акта о проверке остается в проверяемом структурном подразделении.

Результаты проверок подразделений периодически обобщаются Ответственным и доводятся до руководителей подразделений. При необходимости принятия решений по результатам проверок подразделений руководителю Общества готовятся соответствующие служебные записки.

# Приложение №9

к положению о порядке обработки

персональных данных

**Дополнительное соглашение № \_\_\_\_\_\_
к договору от "\_\_\_" \_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_ года № \_\_\_\_\_\_\_\_\_**

|  |  |
| --- | --- |
| \_\_\_\_\_\_\_\_\_\_\_\_ | "\_\_\_" \_\_\_\_\_\_\_\_\_\_\_\_ 201\_ года |

ООО «Ромашка», в лице \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, действующего на основании \_\_\_\_\_\_\_\_\_\_, именуемое в дальнейшем "Заказчик", с одной стороны, и \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, в лице \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, действующего на основании \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, именуемое в дальнейшем "Исполнитель", с другой стороны, совместно именуемые "Стороны", заключили настоящее дополнительное соглашение о нижеследующем:

Дополнить договор от "\_\_\_\_" \_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_ года № \_\_\_\_\_ разделом следующего содержания:

**Конфиденциальность и безопасность персональных данных.**

1. Вся предоставляемая Сторонами друг другу информация считается конфиденциальной и не подлежит разглашению третьим лицам.

2. Исполнитель обязуется осуществлять обработку персональных данных субъекта Заказчика в соответствии с принципами и правилами обработки персональных данных, предусмотренных Федеральным законом Российской Федерации от 27 июля 2006 года № 152-ФЗ "О персональных данных".

3. Цель обработки персональных данных субъекта Заказчика:

|  |
| --- |
|   |
|   |
| (указать цели обработки) |
|  |

4. Перечень действий (операций) по обработке персональных данных, которые будут совершаться лицом, осуществляющим обработку персональных данных, в рамках поручения: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |
| --- |
|   |
| (указать перечень действий) |

5. Исполнитель вправе осуществлять обработку следующих персональных данных субъекта Заказчика: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |
| --- |
|   |
| (указать категории персональных данных) |
|  |

6. Исполнитель обязуется соблюдать конфиденциальность полученных персональных данных субъекта Заказчика и обеспечить безопасность персональных данных при их обработке.

7. Исполнитель при обработке персональных данных субъекта Заказчика обязуется принимать все необходимые организационные, технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении персональных данных.
 8. Исполнитель обязуется обеспечивать безопасность персональных данных применением таких мер как: определение угроз безопасности персональных данных при их обработке в информационных системах; учёт машинных носителей персональных данных; обнаружение фактов несанкционированного доступа к персональным данным и принятием мер; контроль принимаемых мер по обеспечению безопасности персональных данных и уровня защищённости информационных систем персональных данных; и другие меры.
 9. Стороны принимают все необходимые меры для того, чтобы предотвратить разглашение получаемой информации в рамках настоящего договора. Информация может быть предоставлена третьим лицам только в порядке, установленным действующим законодательством Российской Федерации.
 10. Настоящее дополнительное соглашение является неотъемлемой частью договора от "\_\_\_" \_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_ года № \_\_\_\_\_\_\_\_\_, составлено в двух экземплярах, имеющих одинаковую юридическую силу, по одному экземпляру для каждой из Сторон.
 11. Дополнительное соглашение вступает в силу с момента подписания настоящего соглашения Сторонами.

**АДРЕСА И РЕКВИЗИТЫ СТОРОН**

# Приложение №10

к положению о порядке обработки

персональных данных

1. **Задачи ответственного за организацию обработки персональных данных**

На ответственного за организацию обработки персональных данных возложены следующие задачи:

* 1. Организация внутреннего контроля за соблюдением работниками Общества норм законодательства Российской Федерации по обработке персональных данных, в том числе требований, предъявляемых к защите персональных данных. Инструкция по осуществлению внутреннего контроля выполнения требований по защите персональных данных приведена в приложении №8 к настоящему Положению.
	2. Разработка, внедрение и актуализация локальных актов по вопросам обработки персональных данных.
	3. Доведение до сведения работников Общества, непосредственно осуществляющих обработку персональных данных, положений законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных, и проведение обучения указанных работников.
	4. Осуществление контроля приёма и обработки обращений и запросов субъектов персональных данных или их законных представителей по вопросам обработки персональных данных и внесение предложений по организации приёма и обработки таких обращений и запросов.
	5. Осуществление рассмотрения обращений и запросов субъектов персональных данных или их законных представителей по вопросам обработки персональных данных и организация предоставления субъектам персональных данных или их законным представителям информации, предусмотренной Федеральным законом Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных».
	6. Участие совместно с ответственным за защиту информации в Обществе в организации комплексной защиты объектов информатизации Общества, а именно:
1. информационных ресурсов, представленных в виде документированной информации на магнитных, оптических носителях, информативных физических полей, информационных массивов и баз данных, содержащих персональные данные субъектов Общества;
2. средств и систем информатизации (средств вычислительной техники, информационно-вычислительных комплексов, локальных вычислительных сетей и корпоративных информационных систем), программных средств (операционных систем, систем управления базами данных, другого общесистемного и прикладного программного обеспечения), автоматизированных систем управления информационными, управленческими и технологическими процессами, систем связи и передачи данных, технических средств приёма, передачи и обработки информации (звукозаписи, звукоусиления, звуковоспроизведения, переговорных устройств и других технических средств обработки графической, смысловой и буквенно-цифровой информации), используемых для реализации процессов ведения деятельности, обработки информации, содержащей персональные данные субъектов Общества.
	1. Организация совместно с ответственным за защиту информации в Обществе защиты персональных данных субъектов Общества.
	2. Разработка и проведение организационных мероприятий, обеспечивающих безопасность персональных данных, обрабатываемых в Обществе, своевременное выявление и устранение возможных каналов утечки информации.
	3. Организация проведения работ по технической защите информации на объектах информатизации, в информационно-вычислительных сетях, системах и средствах связи и телекоммуникаций, используемых для обработки персональных данных в Обществе.
	4. Контроль реализация технических мер, обеспечивающих своевременное выявление возможных технических каналов утечки персональных данных в подразделениях Общества.
	5. Методическое руководство системой обеспечения информационной безопасности персональных данных Общества.
	6. Организация контроля состояния и проведения оценки эффективности системы обеспечения информационной безопасности персональных данных, а также реализация мер по её совершенствованию.
3. **Функции ответственного за организацию обработки персональных данных.**

Для решения поставленных задач ответственный за организацию обработки персональных данных осуществляет следующие функции:

* 1. Участие в разработке и внедрении правовых, организационных и технических мер по комплексному обеспечению безопасности персональных данных.
	2. Контроль обеспечения соблюдения режима конфиденциальности при обработке персональных данных и внесение предложений по соблюдению такого режима.
	3. Разработка планов по защите персональных данных на объектах Общества.
	4. Контроль выполнения мер по защите персональных данных, анализ материалов контроля, выявление недостатков и нарушений. Разработка и реализация мер по их устранению.
	5. Участие во взаимодействии с контрагентами по вопросам организации и проведения проектно-изыскательских, научно-исследовательских, опытно-конструкторских и других работ по защите информации. Участие в разработке технических заданий на выполняемые исследования и работы.
	6. Контроль выполнения плановых заданий, договорных обязательств, а также сроков, полноты и качества работ по защите персональных данных, выполняемых контрагентами.
	7. Разработка и внесение предложений по обеспечению финансирования работ по защите персональных данных, в том числе выполняемых по договорам.
	8. Участие в проведении работ по технической защите персональных данных на объектах информатизации Общества. Участие в оценке эффективности принятых мер по технической защите информации.
	9. Внесение предложений по выбору, установке, настройке и эксплуатации средств защиты информации, используемых для защиты персональных данных, в соответствии с организационно-распорядительной и эксплуатационной документацией.
	10. Контроль организации режима обеспечения безопасности помещений, в которых происходит обработка персональных данных, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в такие помещения, а также внесение предложений по обеспечению безопасности таких помещений.
	11. Участие в организации доступа работников Общества к персональным данным в соответствии с возложенными на них трудовыми обязанностями и подготовка предложений по организации такого доступа.
	12. Участие в разработке и внедрении локальных актов, определяющих перечень работников Общества, имеющих доступ к персональным данным.
	13. Контроль размещения устройств ввода (отображения) персональных данных, исключающего ее несанкционированный просмотр.
	14. Участие в проведении оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения законодательства по защите персональных данных.
	15. Участие в разработке и реализации политики по работе с инцидентами информационной безопасности в части персональных данных.
	16. Внесение предложений по актуализации внутренней организационно-распорядительной документации по защите персональных данных при изменении существующих и выходе новых нормативных правовых документов по вопросам обработки персональных данных и подготовка или участие в подготовке соответствующих необходимых проектов документов.
1. **Права ответственного за организацию обработки персональных данных**

Ответственный за организацию обработки информации имеет право:

* 1. Осуществлять контроль за деятельностью структурных подразделений Общества по выполнению ими требований по защите персональных данных.
	2. Составлять акты, докладные записки, отчёты для рассмотрения руководством Общества, при выявлении нарушений порядка обработки персональных данных.
	3. Принимать необходимые меры при обнаружении несанкционированного доступа к персональным данным как работниками Общества, так и третьими лицами, и докладывать о принятых мерах руководителю Общества с предоставлением информации о субъектах, нарушивших режим доступа.
	4. Вносить на рассмотрение руководителя Общества предложения, акты, заключения о приостановлении работ в случае обнаружения каналов утечки (или предпосылок к утечке) информации ограниченного доступа.
	5. Давать структурным подразделениям Общества, а также отдельным специалистам обязательные для исполнения указания по вопросам, входящим в компетенцию Ответственного.
	6. Запрашивать и получать от всех структурных подразделений Общества сведения, справочные и другие материалы, необходимые для осуществления деятельности Ответственного.
	7. Составлять, как самостоятельно, так и в составе комиссии, акты и другую техническую документацию о степени защищенности объектов информатизации задействованных в обработке персональных данных.
	8. Готовить и вносить предложения на проведение работ по защите персональных данных; о привлечении к проведению работ по оценке эффективности защиты персональных данных на объектах Общества (на договорной основе) учреждений и организаций, имеющих лицензию на соответствующий вид деятельности; о закупке необходимых технических средств защиты и другой спецтехники, имеющих в обязательном порядке сертификат качества.
	9. Осуществлять визирование договоров с контрагентами с целью правового обеспечения передачи им персональных данных субъектов Общества в ходе выполнения работ по этим договорам.
	10. Представлять интересы Общества при осуществлении государственного контроля и надзора за обработкой персональных данных Уполномоченным органом по защите прав субъектов персональных данных.
1. **Взаимодействия (служебные связи) ответственного за организацию обработки персональных данных**
	1. Ответственный выполняет свои задачи осуществляя взаимодействие со всеми структурными подразделениями Общества.
	2. Для выполнения своих функций и реализации предоставленных прав Ответственный взаимодействует с территориальными и региональными подразделениями Федеральной службы по техническому и экспортному контролю России, Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций, Федеральной службы безопасности Российской Федерации, Министерства внутренних дел Российской Федерации и другими представителями исполнительной власти Российской Федерации и организациями, предоставляющими услуги и выполняющими работы в области защиты персональных данных на законном основании.

**ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| № п/п | Основание для изменений (дата, № документа) | Номера листов | Дата внесе-ния измене-ний | Дата введе-ния измене-ний в дейст-вие | Всего листов в доку-менте | Фамилия лица, ответственного за внесение изменений |
| Изменен-ных | Новых | Анну-ли-рован-ных |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |

1. Функции ответственного определены в Политике информационной безопасности ООО «Ромашка» [↑](#footnote-ref-1)
2. ч.2 ст. 16 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных» [↑](#footnote-ref-2)
3. Пункт 9 части 1 статьи 6 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных» [↑](#footnote-ref-3)
4. Мера ЗИС.3 «Обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи» определена для всех уровней защищенности ИСПДн в документе «Обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи», утвержденном приказом ФСТЭК России от 18.02.2013г. №21 [↑](#footnote-ref-4)
5. Часть 3 статьи 20 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных» [↑](#footnote-ref-5)