



«УТВЕРЖДАЮ»  
Директор ООО «ПК ФОРТУНА»  
А.Н. Топилин  
20 д/г.

15 «Фортуна»

Российская  
Федерация  
Костромская  
область  
г. Середняя Кострома  
ФОТО  
ИИН 4414000370  
ОГРН 1114427000523  
Костромской район

## ПОЛИТИКА

защиты и обработки персональных данных в  
Обществе с ограниченной ответственностью  
«ПРОИЗВОДСТВЕННАЯ КОМПАНИЯ ФОРТУНА»

д. Середняя Костромской р-н, Костромская обл., 2021

## **1. Общие положения.**

1.1. Настоящая Политика Общества с ограниченной ответственностью «ПРОИЗВОДСТВЕННАЯ КОМПАНИЯ ФОРТУНА» в отношении защиты и обработки персональных данных (*далее — Политика защиты и обработки Пдн*), разработана в целях:

- ✓ обеспечения защиты прав и свобод человека и гражданина;
- ✓ определения порядка обработки и защиты персональных данных работников Организации и иных субъектов персональных данных, персональные данные которых подлежат обработке, на основании полномочий компании;
- ✓ защиты прав 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

1.2. Данное Положение разработано в соответствии:

- ✓ Конституцией РФ;
- ✓ Федеральным законом от 19 декабря 2005 г. N 160-ФЗ "О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных";
- ✓ Федеральным законом от 27.07.2006 N 152-ФЗ "О персональных данных";
- ✓ Гражданским Кодексом РФ;
- ✓ Трудовым Кодексом РФ;
- ✓ Налоговым Кодексом РФ;
- ✓ Федеральным законом от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- ✓ Федеральным законом Федеральный закон от 06.12.2011 N 402-ФЗ "О бухгалтерском учете";
- ✓ Указом Президента РФ от 6 марта 1997 г. N 188 "Об утверждении перечня сведений конфиденциального характера";
- ✓ Постановлением Правительства РФ от 15.09.2008 N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляющейся без использования средств автоматизации";
- ✓ Постановлением Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных";
- ✓ Постановлением Правительства РФ от 6 июля 2008 г. N 512 "Об утверждении требований к материальным носителям биометрических

персональных данных и технологиям хранения таких данных вне информационных систем персональных данных";

- ✓ Приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 5 сентября 2013 г. N 996 "Об утверждении требований и методов по обезличиванию персональных данных";
- ✓ Приказом Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. N 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных";
- ✓ и другими нормативными правовыми актами, действующими на момент разработки данной Политики.

1.3. Политика действует в отношении всех персональных данных, которые обрабатывает Общество с ограниченной ответственностью «ПРОИЗВОДСТВЕННАЯ КОМПАНИЯ ФОРТУНА» (далее — *Оператор, ООО «ПК ФОРТУНА», Организация*).

1.4. Политика подлежит опубликованию на сайте Организации для обеспечения неограниченного доступа к документу, определяющему его политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных.

1.5. Субъекты персональных данных, чьи данные обрабатываются Организацией должны ознакомиться самостоятельно с данной Политикой, размещенной на корпоративном сайте.

1.6. Положения Политики служат основой для разработки локальных нормативных актов, регламентирующих в Обществе с ограниченной ответственностью «ПРОИЗВОДСТВЕННАЯ КОМПАНИЯ ФОРТУНА» вопросы обработки персональных данных работников ООО «ПК ФОРТУНА» и других субъектов персональных данных, а также порядка реализации мер для защиты обрабатываемых персональных данных.

1.7. Ответственность за создание системы по соблюдению законодательства по защите персональных данных несет директор Организации.

1.8. Ответственность за соблюдение требований законодательства, данной Политики и иных локальных актов Организации, регулирующих порядок обработки персональных данных несут должностные лица Организации в пределах своих полномочий по обработке персональных данных.

1.9. Данная Политика вступает в действие с даты ее утверждения Директором и действует до его отмены.

## **2. Термины, определения и принятые сокращения.**

В целях настоящего Политики защиты и обработки ПДн используются следующие основные понятия:

- **ООО «ПК ФОРТУНА»** (далее – Компания, Работодатель) – Общество с ограниченной ответственностью **«ПРОИЗВОДСТВЕННАЯ КОМПАНИЯ ФОРТУНА»**, действующее на основании Устава с соблюдением требований действующего российского законодательства;
- **оператор** (далее – Оператор) - ООО «ПК ФОРТУНА», самостоятельно или совместно с другими юридическими и физическими лицами организующее и (или) осуществляющее обработку персональных данных, а также определяющее цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;
- **персональные данные** (далее ПДн) – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);
- **субъект персональных данных** – физическое лицо, чьи персональные данные обрабатывает Оператор;
- **работник** (далее – работник, Работник) – физическое лицо, заключившее трудовой договор с Работодателем;
- **кандидат** (соискатель) (далее – Кандидат) – физическое лицо, выразившее своими действиями желание, чтобы его кандидатура была рассмотрена Работодателем для трудоустройства в Организацию;
- **деловой партнер** – физическое лицо, индивидуальный предприниматель или юридическое лицо, которое заключает с компанией любой гражданско-правовой договор (т. е. совершает сделку). Организация в данной сделке может выступать как Заказчик или как Исполнитель, это не меняет отнесения данного лица к категории Деловой партнер.

К ним отнесены, в частности:

- дистрибуторы;
- контрагенты;
- государственные учреждения;
- иные физические лица, индивидуальные предприниматели или юридические лица, заключившие гражданско-правовой договор с Организацией;
- **должностные лица** – работники Организации, уполномоченные осуществлять обработку ПД субъектов персональных данных и несущие все установленные законодательством виды ответственности за нарушение порядка обработки и сохранности ПД;

- **локальные нормативные акты** (далее – ЛНА) – акты Работодателя, содержащие нормы трудового права, в пределах своей компетенции в соответствии с трудовым законодательством и иными нормативными правовыми актами, содержащими нормы трудового права, коллективными договорами, соглашениями;
- **обработка персональных данных** - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая:
  - сбор;
  - запись;
  - систематизацию;
  - накопление;
  - хранение;
  - уточнение (обновление, изменение),
  - извлечение;
  - использование;
  - передачу (распространение, предоставление, доступ);
  - обезличивание;
  - блокирование;
  - удаление;
  - уничтожение персональных данных;
- **общедоступные источники персональных данных** - источники персональных данных (в том числе справочники, адресные книги), к которым не ограничен доступ третьих лиц и Работников Организации. В общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, сообщаемые субъектом персональных данных;
- **биометрические персональные данные** – сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются Организацией для установления личности субъекта персональных данных, к ним относится, в частности, фото, видеоизображение субъекта персональных данных;
- **автоматизированная обработка персональных данных** - обработка персональных данных с помощью средств вычислительной техники;

- **распространение персональных данных** - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;
- **предоставление персональных данных** - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;
- **блокирование персональных данных** - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);
- **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;
- **обезличивание персональных данных** - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;
- **информационная система персональных данных** - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;
- **угроза безопасности персональных данных** - совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных;
- **уровень защищенности персональных данных** - комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
- **трансграничная передача персональных данных** - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу;
- **технические средства, позволяющие осуществлять обработку персональных данных** – специальное оборудование, к которому относятся:
  - средства вычислительной техники,
  - информационно-вычислительные комплексы и сети,

- средства и системы передачи, приема и обработки ПД (*средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие средства обработки речевой, графической и буквенно-цифровой информации*),
- программные средства (*операционные системы, системы управления базами данных и прочее*),
- средства защиты информации, применяемые в информационных системах.

### **3. Цели обработки персональных данных**

3.1. Обработка персональных данных субъектов в ООО «ПК ФОРТУНА» осуществляется исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов Российской Федерации.

Обработка Оператором персональных данных осуществляется в следующих целях:

- ✓ осуществление деятельности в соответствии с Уставом ООО «ПК ФОРТУНА»;
- ✓ ведение кадрового делопроизводства и бухгалтерского учета;
- ✓ содействие работникам в трудоустройстве, получении образования и продвижении по службе, обеспечение личной безопасности работников, контроль количества и качества выполняемой работы, обеспечение сохранности имущества;
- ✓ привлечение и отбор кандидатов на работу у Оператора;
- ✓ организация постановки на индивидуальный (персонифицированный) учет работников в системе обязательного пенсионного страхования;
- ✓ заполнение и передача в органы исполнительной власти и иные уполномоченные организации требуемых форм отчетности;
- ✓ исполнения договоров, заключенных с физическими лицами, состоящими в договорных и иных гражданско-правовых отношениях с ООО «ПК ФОРТУНА»;
- ✓ выполнения договорных соглашений с субъектами;
- ✓ проведения акций, опросов, маркетинговых, статистических и иных исследовательских действий;
- ✓ осуществление пропускного режима.

#### **4. Принципы защиты и правила обработки персональных данных в Организации**

4.1. Обработка персональных данных должна осуществляться на законной и справедливой основе.

4.2. Обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных. Цели обработки ПД отражаются в ЛНА по ПДн, с которыми субъект ПДн знакомится до предоставления своих ПДн, а также в письменных согласиях субъектов ПДн (*оформляемых в случае требований законодательства*).

4.3. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой. Для соблюдения данного принципа в Организации применяются различные информационные системы, позволяющие разделить допуск должностных лиц к тем или иным ПДн, а также процедуры допуска к ПДн субъектов, необходимых должностным лицам, для осуществления своих трудовых функций.

4.4. Обработке подлежат только персональные данные, которые отвечают целям их обработки. ПДн, которые Организация имеет право обрабатывать, отражаются в ЛНА по ПДн, с которыми субъект ПД знакомится до предоставления своих ПДн, а также в письменных согласиях субъектов ПД (*оформляемых в случае требований законодательства*).

4.5. Содержание и объем обрабатываемых персональных данных собирается должностными лицами Организации в соответствии с заявленными целями обработки ПДн. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки. В случае предоставления избыточных данных самим субъектом ПДн Организация имеет право:

- ✓ отказать в их принятии;
- ✓ уничтожить в присутствии субъекта ПДн,
- ✓ использовать свои типовые формы по сбору ПДн для исключения сбора избыточных ПДн.

4.6. При обработке персональных данных Организация обеспечивает точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Организация предпринимает необходимые меры либо обеспечивает их принятие по удалению или уточнению неполных или неточных данных.

4.7. Хранение ПДн осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем, по которому является субъект персональных данных.

4.8. Обрабатываемые ПДн уничтожаются либо обезличиваются по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

4.9. Организация для соблюдения требований архивного законодательства знакомит субъекта ПДн со сроками, в течение которых персональные данные, предоставляемые, согласно законодательству, будут храниться в Организации.

4.10. Организация проводит регулярный анализ соответствия процессов обработки ПДн в информационных системах Организации в случае:

- ✓ создания новых информационных систем;
- ✓ внесения изменений в технологические процессы, существующие в информационных системах;
- ✓ изменения нормативной базы, затрагивающей принципы и процессы обработки ПДн в информационных системах Организации .

## **5. Обязанности Организации при сборе и обработке персональных данных**

5.1. При сборе персональных данных ООО «ПК ФОРТУНА» обязана предоставить субъекту персональных данных по его просьбе информацию, касающуюся обработки его персональных данных, в том числе содержащей:

- ✓ подтверждение факта обработки персональных данных Организацией;
- ✓ правовые основания и цели обработки персональных данных;
- ✓ цели и применяемые Организацией способы обработки персональных данных;
- ✓ сведения о лицах (*за исключением работников Организации*), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с ООО «ПК ФОРТУНА» 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;
- ✓ порядок осуществления субъектом персональных данных прав, предусмотренных действующим законодательством;
- ✓ информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- ✓ наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Организации, если обработка поручена или будет поручена такому лицу;
- ✓ иные сведения, предусмотренные действующим законодательством.

5.2. Если предоставление персональных данных является обязательным в соответствии с федеральным законом, Организация обязана разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные.

5.3. Если персональные данные получены не от субъекта персональных данных, Организация, до начала обработки таких персональных данных обязана предоставить субъекту персональных данных следующую информацию:

- ✓ цель обработки персональных данных и ее правовое основание;
- ✓ предполагаемые пользователи персональных данных;
- ✓ установленные законодательством права субъекта персональных данных;
- ✓ источник получения персональных данных.

5.4. Организация освобождается от обязанности предоставить субъекту персональных сведений, предусмотренные п.6.3. Политики, если:

- ✓ субъект персональных данных уведомлен об осуществлении обработки его персональных данных Организацией;
- ✓ персональные данные получены Организацией на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем, по которому является субъект персональных данных;
- ✓ персональные данные сделаны общедоступными субъектом персональных данных или получены из общедоступного источника;
- ✓ Организация осуществляет обработку персональных данных для статистических или иных исследовательских целей, для осуществления научной, литературной или иной творческой деятельности, если при этом не нарушаются права и законные интересы субъекта персональных данных;
- ✓ предоставление субъекту персональных данных сведений, нарушает права и законные интересы третьих лиц.

5.5. При сборе персональных данных, в том числе посредством информационнотелекоммуникационной сети "Интернет", Организация обязана обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, прямо предусмотренных законодательством.

5.6. Организация обязана при получении соответствующего запроса 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.

5.7. 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, Организация обязана внести в них необходимые изменения.

5.8. 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, Организация обязана уничтожить такие персональные данные.

5.9. Организация обязана 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.

5.10. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя либо по запросу субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных Организация обязана осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (*если обработка персональных данных осуществляется другим лицом, действующим по поручению Организации*) с момента такого обращения или получения указанного запроса на период проверки.

5.11. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных Организация обязана осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (*если обработка персональных данных осуществляется другим лицом, действующим по поручению Компании*) с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

5.12. В случае подтверждения факта неточности персональных данных Организация на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязана уточнить персональные данные либо обеспечить их уточнение (*если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора*) в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

5.13. В случае выявления неправомерной обработки персональных данных, осуществляющей Организацией или лицом, действующим по поручению Организации, ООО «ПК ФОРТУНА» в срок, не превышающий трех рабочих дней с даты этого выявления, обязана прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению Организации.

5.14. В случае, если обеспечить правомерность обработки персональных данных невозможно, Организация в срок, не превышающий десяти рабочих дней с

даты выявления неправомерной обработки персональных данных, обязана уничтожить такие персональные данные или обеспечить их уничтожение.

5.15. Об устраниении допущенных нарушений или об уничтожении персональных данных Организация обязана уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

5.16. В случае достижения цели обработки персональных данных Организация обязана прекратить обработку персональных данных или обеспечить ее прекращение (*если обработка персональных данных осуществляется другим лицом, действующим по поручению Организации*) и уничтожить персональные данные или обеспечить их уничтожение (*если обработка персональных данных осуществляется другим лицом, действующим по поручению Организации*) в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между Организацией и субъектом персональных данных либо если Организация не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных действующим законодательством.

5.17. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных Организация обязана прекратить их обработку или обеспечить прекращение такой обработки (*если обработка персональных данных осуществляется другим лицом, действующим по поручению Компании*) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные или обеспечить их уничтожение (*если обработка персональных данных осуществляется другим лицом, действующим по поручению Компании*) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между Организацией и субъектом персональных данных либо если Организация не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных действующим законодательством.

5.18. В случае отсутствия возможности уничтожения персональных данных в течение установленного срока, Организация осуществляет блокирование таких персональных данных или обеспечивает их блокирование (*если обработка персональных данных осуществляется другим лицом, действующим по поручению Компании*) и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен действующим законодательством.

## 6. Организация и контроль обеспечения защиты персональных данных

6.1. Организация предпринимает меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных действующим законодательством.

6.2. Организация самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных законодательством.

Для реализации мер защиты персональных данных Организация:

- ✓ назначает ответственных за организацию обработки персональных данных;
- ✓ издает локальные нормативные акты, определяющих политику ООО «ПК ФОРТУНА» в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;
- ✓ применяет правовые, организационные и технические меры по обеспечению безопасности персональных данных;
- ✓ осуществляет внутренний контроль и (или) аудит соответствия обработки персональных данных требованиям действующего законодательства, требованиям к защите персональных данных, политике Организации в отношении обработки персональных данных, локальным актам Организации;
- ✓ оценивает вред, который может быть причинен субъектам персональных данных в случае нарушения требований действующего законодательства, соотношение указанного вреда и принимаемых Организацией мер, направленных на обеспечение выполнения обязанностей, предусмотренных законодательством;
- ✓ знакомит работников Организации, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику Компании в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.

6.3. Система защиты персональных данных является частью общей системы обеспечения информационной безопасности Организации.

6.4. Ответственность за создание системы защиты персональных данных, обрабатываемых в Организации, несет директор.

6.5. Лица, ответственные за функционирование информационной системы несут ответственность за необеспечение сохранности и защиты персональных данных, обрабатываемых в информационных системах.

6.6. Общий контроль за соблюдением законодательства и Политики осуществляют начальник отдела по управлению кадрами и трудовыми отношениями.

6.7. Руководители структурных подразделений несут ответственность за соблюдение установленных в Организации требований по защите персональных данных работников своего подразделения.

6.8. Руководители структурных подразделений получают указания непосредственно от директора и подотчетно по вопросам организации процесса обработки персональных данных данным лицам.

6.9. Руководители структурных подразделений, в частности, обязаны:

- ✓ осуществлять внутренний контроль за соблюдением работниками структурного подразделения законодательства Российской Федерации о персональных данных, локальных нормативных актов, включая данную Политику по вопросам защиты персональных данных;
- ✓ доводить до сведения Работников структурного подразделения положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;
- ✓ организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

6.10. Должностные лица (Работники Организации), допущенные к обработке персональных данных, несут персональную ответственность за соблюдение требований локальных нормативных актов Организации по работе с персональными данными лиц, к обработке которых допущено данное должностное лицо.

6.11. Принципы и требования по обеспечению безопасности ПДн распространяются на все возможные формы существования информации, такие как:

- ✓ физические поля (*электрические, акустические, электромагнитные, оптические и т. п.*);
- ✓ носители (*электронные – магнитные и оптические (CD и DVD) накопители, съемные жесткие диски и флэш-накопители, бумажные носители*);
- ✓ на все возможные форматы представления ПДн такие как:
  - документы;
  - голос;
  - изображения;
  - файлы;
  - почтовые сообщения;

- базы данных;
- записи базы данных;
- другие информационные массивы.

6.12. Целью создания системы защиты ПДн является исключение неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения ПДе, а также иных неправомерных действий, путем обеспечения:

- конфиденциальности;
- целостности;
- доступности;
- невозможности отказа от авторства;
- учета;
- аутентичности;
- адекватности.

6.13. Предотвращение несанкционированного (*в том числе и случайного*) и незаконного доступа к информационным системам, технологиям и информационным ресурсам, результатом которого может стать уничтожение, модификация, искажение, копирование, распространение, блокирование ПДн требует применения комплекса правовых, организационных, организационно-технических мер защиты с использованием сертифицированных средств защиты информации.

6.14. К основным задачам в области обеспечения безопасности ПДн относится:

- ✓ определение актуальных угроз безопасности ПДн и информационных технологий, используемых в информационных системах;
- ✓ применение организационных и технических мер по обеспечению безопасности ПДн при их обработке в информационных системах, необходимых для выполнения требований к защите ПДн данных, исполнение которых обеспечивает установленные законодательством уровни защищенности ПДн;
- ✓ применение процедур оценки соответствия средств защиты информации;
- ✓ оценка эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию информационной системы;
- ✓ учет машинных носителей ПДн;
- ✓ обеспечение работоспособного функционирования компьютерной техники с ПДн в соответствии с эксплуатационной и технической документацией компьютерной техники и с учетом технических требований информационных систем и средств защиты информации;
- ✓ обнаружение и регистрация фактов несанкционированного доступа к ПДн, несанкционированной повторной и дополнительной записи

информации после ее извлечения из информационной системы ПД и принятие мер;

- ✓ разработка (актуализация) документации на систему защиты ПДн;
- ✓ сертификация применяемых средств защиты информации;
- ✓ выбор и внедрение необходимых и достаточных мер и средств защиты ПДн;
- ✓ эксплуатация системы защиты ПДн в соответствии с документацией на нее;
- ✓ учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;
- ✓ восстановление ПДн, модифицированных или удаленных, уничтоженных вследствие несанкционированного доступа к ним;
- ✓ установление правил доступа к ПДн, обрабатываемым в информационной системе Организации, а также обеспечение регистрации и учета всех действий, совершаемых с ПДн в информационной системе;
- ✓ контроль за принимаемыми мерами по обеспечению безопасности ПДн и уровней защищенности информационных систем;
- ✓ сбор согласий на обработку ПДн с субъектов ПД в случаях, установленных законодательством;
- ✓ разработка и актуализация Перечня персональных данных обрабатываемых в Организации;
- ✓ контроль целей обработки ПДн, соответствия обрабатываемых ПДн целям обработки;
- ✓ уничтожение ПДн в установленном порядке;
- ✓ оптимизация информационных и бизнес-процессов обработки ПДн;
- ✓ управление взаимодействиями с внешними контрагентами по вопросам обработки ПДн;
- ✓ взаимодействие с субъектами ПДн по вопросам обработки их ПДн;
- ✓ контроль уровня защищенности ПДн;
- ✓ обучение персонала по вопросам защиты ПДн;
- ✓ учет лиц, допущенных к обработке ПДн;
- ✓ взаимодействие с регулирующими органами по вопросам защиты ПДн;
- ✓ реагирование на нештатные ситуации, расследование нештатных ситуаций возникающих при обработке ПДн;

6.15. Запрещается вынос (вывоз) документов, электронных или иных носителей ПДн, а также их передача лицам, не допущенным к обработке ПДн, без согласования с ответственным за обеспечение безопасности ПДн Организации.

6.16. При выносе устройств, хранящих ПДн, за пределы контролируемой зоны для ремонта, замены и т. п. должно быть обеспечено гарантированное уничтожение информации, хранимой на этих устройствах.

6.17. Копирование и составление выписок из документов, содержащих ПДн разрешается исключительно в служебных целях с письменного разрешения руководителя структурного подразделения.

6.18. Обслуживание помещения (*уборка или различный ремонт помещения, инженерно-технического оборудования*) проводится обслуживающим персоналом только в присутствии и под присмотром хотя бы одного из Работников, имеющего право самостоятельно находиться в помещении. В случае если возможность присмотра отсутствует, то носители информации персональных данных должны быть защищены от несанкционированного доступа (*например, путем организации видеонаблюдения в помещении, размещения носителей только в запираемых шкафах и др. способами, обеспечивающими несанкционированный доступ или контроль за рисками такого доступа*).

6.19. Работники подразделения, обеспечивающие контроль действий обслуживающего персонала в помещении, обязаны не допускать несанкционированных действий в отношении информационной системы, бумажных и магнитных носителей информации, компонентов инженерных систем и т. п., содержащих ПДн.

6.20. Капитальный и/или иной ремонт, продолжительный по времени и требующий высвобождения рабочей площади помещения, может проводиться и без присмотра, однако при этом в обязательном порядке:

- ✓ носители информации должны быть вынесены из ремонтируемого помещения в другое контролируемое помещение;
- ✓ по окончанию ремонта должны быть сменены ключи и коды доступа в помещение.

6.21. Для сохранения целостности и доступности ПДн, а также для обеспечения непрерывности бизнес-процессов связанных с обработкой ПДн, Организация организовывает мероприятия по резервному копированию ПДн.

## 7. Права субъектов персональных данных

7.1. Субъект персональных данных имеет право:

- ✓ на доступ к его персональным данным;
- ✓ на получение информации, касающейся обработки его персональных данных;
- ✓ на обжалование действий или бездействий Организации.

7.2. Субъект персональных данных вправе требовать от Организации уточнения его 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.

7.3. Субъект ПДн имеет право отправить в Организацию запрос на предоставление необходимых субъекту ПДн сведений, содержащих информацию об обработке его ПД. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с Организацией (*номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения*), либо сведения, иным образом подтверждающие факт обработки персональных данных Организацией, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

7.4. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

- ✓ подтверждение факта обработки персональных данных Организацией;
- ✓ правовые основания и цели обработки персональных данных;
- ✓ цели и применяемые Организацией способы обработки персональных данных;
- ✓ сведения о лицах (за исключением работников Организации), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Компанией 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;
- ✓ порядок осуществления субъектом персональных данных прав, предусмотренных настоящим Федеральным законом;
- ✓ информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- ✓ наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Организации, если обработка поручена или будет поручена такому лицу;
- ✓ иные сведения, предусмотренные действующим законодательством.

7.5. 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.

7.6. Обработка персональных данных в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи, допускается только при условии предварительного согласия субъекта персональных данных.

7.7. 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 или в случаях, предусмотренных федеральными законами, устанавливающими также меры по обеспечению соблюдения прав и законных интересов субъекта персональных данных.

7.8. Если субъект персональных данных считает, что Организация осуществляет обработку его персональных данных с нарушением требований действующего законодательства или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие Организации в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

7.9. Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

## **8. Система локальных нормативных актов по защите персональных данных Организации**

8.1. Система локальных нормативных актов - совокупность локальных нормативных актов Организации, описывающих порядок обработки персональных данных должностными лицами Организации.

8.2. Система ЛНА состоит из следующих актов:

- ✓ Данная Политика,
- ✓ Положение по защите ПДн работников и лиц, чьи данные обрабатываются в связи с трудовыми отношениями с Работодателем,
- ✓ Положение по защите ПДн субъектов, чьи данные обрабатываются в связи с деловыми бизнес-отношениями с Организацией.

8.3. Организация может в рамках своих полномочий издавать и иные локальные нормативные акты, положения, инструкции, которые будут регулировать отдельные вопросы обработки персональных данных, обязанности и права отдельных структурных подразделений и должностных лиц.

8.4. Ответственные должностные лица за работу с ПДн определяются в отдельных ЛНА, указанных в п.6.2. данной Политики, а также в иных локальных актах и распорядительных документах Организации.

8.5. Субъекты ПДн, перечень ПДн, которые имеет право обрабатывать Организация, действия, которые осуществляются с ПДн, определяются:

- ✓ законодательством РФ,
- ✓ ЛНА, входящими в систему ЛНА по ПДн,
- ✓ письменными согласиями субъектов ПДн.

8.6. При изменении законодательства локальные нормативные акты, составляющие систему ЛНА по ПДн Организации применяются в нормах, не противоречащих законодательству. Положения ЛНА, противоречащие законодательству, в том числе, в случае его изменения, не могут быть основанием для предъявления претензий со стороны субъектов ПДн. Организация несет ответственность только в случае осуществления незаконных действий, ущемляющих права субъекта ПДн.