ПОЛИТИКА ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Утверждена приказом ООО «Микроолап текнолоджис»
№ 20240110-5 от 10 января 2024г.

1. Общие положения

1.1. Настоящая Политика обработки персональных данных (далее — Политика) определяет цели и общие принципы обработки персональных данных (далее ПДн), а также реализуемые меры защиты прав субъектов ПДн в ООО «Микроолап текнолоджис».

Политика действует в отношении всех ПДн, которые обрабатывает ООО «Микроолап текнолоджис» (далее Оператор).

1.2. Политика распространяется на отношения в области обработки ПДн, возникшие у Оператора как до, так и после утверждения настоящей Политики.

1.3. Меры по охране баз данных, содержащих ПДн, принимаемые Оператором, включают в себя:

- определение перечня информации, составляющей ПДн;
- ограничение доступа к информации, содержащей ПДн, путём установления порядка обращения с этой информацией и контроля за соблюдением такого порядка.

1.4. Меры по охране конфиденциальности информации признаются разумно достаточными, если:

- исключается доступ к ПДн любых третьих лиц без согласия Оператора;
- обеспечивается возможность использования информации, содержащей ПДн, без нарушения законодательства о ПДн;
- при работе с Пользователем устанавливается такой порядок действий Оператора, при котором обеспечивается сохранность сведений, содержащих ПДн Пользователя.

2. Правовая основа

2.1. Настоящая Политика ООО «Микроолап текнолоджис» в отношении обработки ПДн разработана во исполнение требований пункта 2 части 1 статьи 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О Персональных данных» (далее – Закон 152-ФЗ) в целях обеспечения защиты прав и свобод человека и гражданина при обработке его ПДн, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну и непрерывное развитие и совершенствование системы информационной безопасности (далее ИБ).

2.2. Во исполнение требований части 2 статьи 18.1 Закона 152-ФЗ о ПДн настоящая Политика является общедоступным документом ООО «Микроолап текнолоджис» и предусматривает возможность ознакомления любых лиц с ней в сети интернет по адресу https://www.microolap.ru/privacy/ путём скачивания pdf-файла её действующей версии.

2.3. ПДн не могут быть использованы в целях, противоречащих требованиям Закона 152-ФЗ, защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

3. Список ролей

К обработке ПДн допускаются работники ООО «Микроолап текнолоджис» согласно утверждённого оператором перечня лиц, доступ которых к ПДн, обрабатываемых в информационной системе (далее ИС) ООО «Микроолап текнолоджис», необходим для выполнения ими служебных (трудовых) обязанностей;

Организацию обработки ПДн, а также обеспечение мер защиты прав субъектов ПДн в ООО «Микроолап текнолоджис», в том числе обеспечение соблюдения требований настоящей Политики осуществляют:

- Ответственный за обработку персональных данных: работник, назначенный лицом, ответственным за обработку персональных данных, и обеспечивающий организационно-правовую защиту ПДн в ООО «Микроолап текнолоджис» в соответствии с требованиями законодательства в области ПДн.
- Ответственный по организационному и документационному обеспечению управления организацией, включая ведение кадрового учёта; создание и использование электронных документов (ЭД), составление и ведение электронного документооборота (ЭДО); включая ведение кадрового электронного документооборота (КЭДО); хранение и обработку бумажных и электронных документов (ЭД).
- Ответственный за организацию работ по криптографической защите информации: работник, ответственный за организацию использование средств криптографической защиты информации; оборудование и защиту от несанкционированного доступа рабочего места, магнитных носителей криптографических ключей, архивов ЭД.
- Ответственный за информационную безопасность - работник, назначенный лицом, ответственным за обеспечение информационной безопасности (ИБ) в целом по Организации; за предупреждение хакерских атак, разработку и реализацию стратегии кибербезопасности в соответствии с бизнес-целями компании и требованиями регулирующих органов, а также взаимодействие с Роскомнадзором по этим вопросам.

4. Основные принципы организации и обработки персональных данных

ООО «Микроолап текнолоджис» организует и осуществляет обработку ПДн, руководствуясь следующими принципами:

- осуществления обработки ПДн на законной и справедливой основе в соответствии с требованиями нормативных правовых актов (Приложение 2);
- источником информации о ПДн сотрудников является непосредственно сам сотрудник;
- источником информации о ПДн сотрудников являются сведения, полученные вследствие предоставления Оператором сотруднику прав пользования ИСПДн;
- соблюдения конфиденциальности ПДн в соответствии с требованиями действующего законодательства; ПДн сотрудников относятся к конфиденциальной информации ограниченного доступа;
- обработке подлежат только ПДн, которые отвечают целям их обработки;
- недопустимости объединения баз данных (далее БД), содержащих ПДн, обработка которых осуществляется в несовместимых между собой целях;
- недопустимости обработки ПДн, которые являются избыточными по отношению к заявленным целям их обработки;
- обеспечения точности и достаточности ПДн, а в необходимых случаях также актуальности по отношению к целям обработки соответствующих ПДн;
- хранения ПДн в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели их обработки, если срок хранения ПДн не установлен федеральным законом,

договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн;

- уничтожения или обезличивание ПДн по достижении целей их обработки либо в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом;

- недопущения неправомерного доступа, уничтожения, модификации, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении ПДн;

- передача ПДн органам дознания и следствия, в ФНС, фонд СФР РФ и другие уполномоченные органы исполнительной власти и организации осуществляется в соответствии с требованиями законодательства РФ.

Подтверждение факта обработки ПДн ООО "Микроолап текнолоджис", правовые основания и цели обработки ПДн, а также иные сведения, указанные в части 7 статьи 14 Закона о ПДн, предоставляются ООО "Микроолап текнолоджис" субъекту ПДн или его представителю при обращении либо при получении запроса субъекта ПДн или его представителя.

В предоставляемые сведения не включаются ПДн, относящиеся к другим субъектам ПДн, за исключением случаев, когда имеются законные основания для раскрытия таких ПДн.

4.2. Получение Согласия для обработки ПДн.

Осуществляется в устной и письменной форме непосредственно с письменного согласия субъектов ПДн на обработку их ПДн, а также без такового в случаях, предусмотренных законодательством РФ на следующих условиях:

4.2.1. Согласие на обработку ПДн для публикации на сайте ООО "Микроолап текнолоджис".

4.2.2. Согласие на обработку ПДн при осуществлении основной деятельности в соответствии с Уставом ООО «Микроолап текнолоджис».

4.2.3. Согласие на обработку ПДн для ведения кадрового делопроизводства.

4.2.4. Согласие на обработку ПДн для содействие работникам в трудоустройстве, получении образования, обеспечение личной безопасности работников, контроль количества и качества выполняемой работы, обеспечение сохранности имущества.

4.2.5. Согласие на обработку ПДн для ведения индивидуального (персонифицированного) учёта работников в системе обязательного пенсионного страхования.

4.2.6. Согласие на обработку ПДн для ведение налогового и бухгалтерского учёта.

4.2.7. Согласие на обработку ПДн для заполнения и передача в органы исполнительной власти и иные уполномоченные организации требуемых форм отчётности.

4.2.8. Обработка ПДн в целях продвижение товаров, работ, услуг на рынке путём осуществления прямых контактов с потенциальным потребителем с помощью средств связи осуществляется ООО «Микроолап текнолоджис» только на основании согласия субъекта на обработку его ПДн и прекращается незамедлительно в случае поступления соответствующего требования субъекта ПДн.

4.3. ООО «Микроолап текнолоджис» не осуществляет обработку категорий ПДн:

4.3.1. ООО «Микроолап текнолоджис» не осуществляет обработку специальных категорий ПДн.

4.3.2. ООО «Микроолап текнолоджис» не осуществляет обработку биометрических ПДн.

4.3.3. ООО «Микроолап текнолоджис» не создаёт общедоступных источников ПДн.

4.3.4. ООО «Микроолап текнолоджис» не обрабатывает ПДн для распространения.

5. Цели обработки ООО "Микроолап текнолоджис" персональных данных и категории субъектов персональных данных

5.1. ООО "Микроолап текнолоджис" ПДн осуществляет обработку ПДн в следующих целях:

- Обеспечение соблюдения Конституции, федеральных законов и иных нормативных правовых актов Российской Федерации;
- Осуществление деятельности в соответствии с Уставом ООО «Микроолап текнолоджис»;
- Организация, обеспечение и осуществление договорной работы с клиентами Общества;
- Продвижение работ и услуг Общества на рынке, в том числе организация и проведение маркетинговых и иных мероприятий; предоставление консультаций, материалов и сведений по продуктам и сервисам, а также иным направлениям деятельности Общества;
- Организация и осуществление внешнего и внутреннего взаимодействия (в том числе поддержание деловых связей и делового общения; обеспечение эффективного информационного взаимодействия; рассмотрение обращений (включая обращения (запросы) субъектов персональных данных); создание и поддержание положительного имиджа (деловой репутации), в том числе путём размещения информации о деятельности Общества, его работниках и иных лицах на информационных ресурсах в информационно-телекоммуникационной (далее ИТК) сети «Интернет» ;
- Ведение кадрового делопроизводства и учёта работников Общества;
- Содействие работникам Общества в трудоустройстве, получении образования, обеспечение личной безопасности, контроль количества и качества выполняемой работы, обеспечение сохранности имущества;
- Привлечение и отбор кандидатов на работу в Обществе;
- Организация постановки на индивидуальный (персонифицированный) учёт работников Общества в системе обязательного пенсионного и социального страхования;
- Организация постановки работников Общества на воинский учёт;
- Заполнение и передача в органы исполнительной власти и иные уполномоченные организации требуемых форм отчётности;
- Осуществление гражданско-правовых отношений;
- Ведение налогового и бухгалтерского учёта;
- Контроль за соблюдением внутренних нормативных документов Общества;
- Обеспечение безопасности и сохранности имущества (в том числе проверка добросовестности и благонадёжности контрагентов (их представителей), работников, кандидатов (соискателей на замещение вакантных должностей);
- Организация безопасности работников и обеспечения пропускного и внутриобъектового режимов.

5.2. ПДн, обрабатываемые ООО "Микроолап текнолоджис":

- данные, полученные при осуществлении основной деятельности ООО "Микроолап текнолоджис";
- данные, полученные для публикации на сайте ООО "Микроолап текнолоджис", включая изображения (фото- и видео-) работников;
- данные, полученные для ведения кадрового делопроизводства;
- данные, полученные при осуществлении трудовых отношений;
- данные, полученные для для ведения индивидуального (персонифицированного) учёта работников в системе обязательного пенсионного страхования;
- данные, полученные для ведение налогового и бухгалтерского учёта;

- данные, полученные при осуществлении гражданско-правовых отношений;
- данные, полученные для осуществления отбора кандидатов на работу;
- данные, полученные для заполнения и передача в органы исполнительной власти и иные уполномоченные организации требуемых форм отчётности.

5.2.1. Материалы видеосъемки, осуществляемой на территории Оператора

Материалы используются с целью организации безопасности работников и обеспечения пропускного и внутриобъектового режимов. Материалы видеосъемки не используются Оператором для установления личностей Субъектов. В соответствии с частью 3 статьи 6 Федерального закона N 152-ФЗ Оператор с целью организации безопасности работников и обеспечения пропускного и внутриобъектового режимов вправе поручить обработку персональных данных другому лицу, в данном случае частной охранной организации, с согласия Субъекта ПДн.

5.3. Категории субъектов ПДн.

Обрабатываются ПДн следующих субъектов ПДн:

- физические лица, состоящие с ООО «Микроолап текнолоджис» в трудовых отношениях;
- физические лица, уволившиеся из ООО «Микроолап текнолоджис»;
- физические лица, состоящие с ООО «Микроолап текнолоджис» в гражданско-правовых отношениях;
- юридические лица, связанные с продвижением работ и услуг ООО «Микроолап текнолоджис» на рынке, в том числе материалов и сведений по продуктам и сервисам, а также иным направлениям деятельности Общества.

6. Способы и сроки обработки персональных данных

6.1. При организации и осуществлении обработки ПДн ООО «Микроолап текнолоджис» устанавливает для каждой цели обработки конкретные сроки обработки и хранения с учётом:

- требований действующего законодательства Российской Федерации;

- условий договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн;

- срока действия данного субъектом ПДн согласия на обработку его ПДн.

6.2. ООО «Микроолап текнолоджис» осуществляет обработку ПДн в течение срока, необходимого для достижения заявленной цели обработки из числа целей обработки ПДн, определённых настоящей Политикой или до утраты необходимости в достижении заявленной цели обработки ПДн, если требование об обработке ПДн свыше указанного срока не установлено действующим законодательством Российской Федерации.

6.3. В случае осуществления обработки ПДн на основании согласия субъекта ПДн ООО «Микроолап текнолоджис» для целей, определённых в настоящей Политики, вправе обрабатывать ПДн в течение указанного в соответствующем согласии срока его действия, но не дольше, чем это необходимо для достижения заявленной цели обработки ПДн, и прекращает осуществляемую на основании согласия обработку ПДн в случае отзыва соответствующего согласия субъектом ПДн.

6.4. Обработка ПДн на основании договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн, осуществляется ООО «Микроолап текнолоджис» в течение срока действия соответствующего договора (в том числе трудового договора, соглашения об использовании сайта, сервиса или продукта (пользовательского соглашения), где применимо для цели, определённой настоящей Политики; иных гражданско-правовых договоров) либо в течение срока, который установлен таким договором.

6.5. Указанные сроки обработки ПДн и (или) правила их установления применимы ко всем целям, определенным ООО «Микроолап текнолоджис» в настоящей Политике.

6.6 Для достижения определённых в настоящей Политике целей обработки ПДн ООО «Микроолап текнолоджис» осуществляет автоматизированную и не автоматизированную (включая смешанную) обработку ПДн посредством совершения в том числе следующих действий (операций) или совокупности действий (операций): *сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение*.

6.7. Перечень информационных систем персональных данных (ИСПДн) операторов, задействованных в обработке ПДн ООО «Микроолап текнолоджис» на ресурсах ИТК сети Интернет:

http://www.microolap.ru - официальный сайт компании ООО Микроолап текнолоджис». ИСПДн «Центр обработки данных (ЦОД) ПДн сотрудников компании»;

http://kedo.kontur.ru - ИСПДн кадрового электронного документа оборота «Контур.КЭДО» АО "ПФ "СКБ КОНТУР" для обмена кадровыми документами между работодателем и сотрудниками ООО Микроолап текнолоджис». Реестр операторов, осуществляющих обработку ПДн, регистрационный номер 09-0066830 от от 05.10.2009.

http://diadoc.kontur.ru - ИСПДн электронного документа оборота «Контур.Диадок» АО "ПФ "СКБ КОНТУР" для обмена электронными документами между ООО Микроолап текнолоджис» и контрагентами;

http://btrx.l7.cx - Программный комплекс «1С-Битрикс24» от компании ООО «Битрикс» для ведения электронного документа оборота и обработки ПДн ООО «Микроолап текнолоджис» и ПДн юридических лиц, связанных с продажей и продвижением продуктов, работ и услуг ООО «Микроолап текнолоджис» на рынке, в том числе материалов и сведений по продуктам и сервисам, а также иным направлениям деятельности Общества. Реестр операторов, осуществляющих обработку ПДн, регистрационный номер 77-18-010056 от от 17.04.2018.

http://tbank.ru - ИСПДн банка АО «ТБанк» для учёта зарплаты, подготовки отчётных сведений ООО «Микроолап текнолоджис» для ФНС и СФР. Реестр операторов, осуществляющих обработку ПДн, регистрационный номер 08-0023207 от от 24.10.2008.

7. Прекращение обработки персональных данных и уничтожение.

7.1. ООО "Микроолап текнолоджис" прекращает обработку ПДн субъектов ПДн,на основании заключённого между ними и ООО "Микроолап текнолоджис" договора в следующих случаях:

- при достижении цели обработки ПДн;
- по истечении срока действия согласия субъекта ПДн;
- при отзыве согласия субъекта ПДн на обработку его ПДн;
- при поступлении ООО "Микроолап текнолоджис" в случаях, предусмотренных законодательством в области ПДн, требования субъекта ПДн о прекращении обработки его ПДн;
- по истечении срока действия договора, стороной которого является субъект ПДн;
- по истечении установленного действующим законодательством Российской Федерации срока обработки ПДн.

7.2. В случаях, указанных в п.7.1. настоящей Политики, ООО "Микроолап текнолоджис" прекращает обработку ПДн в порядке и в сроки, установленные законодательством в области ПДн.

7.3. В случаях, установленных законодательством в области ПДн, ООО "Микроолап текнолоджис" осуществляет посредством совершения действий, в результате которых становится невозможно восстановить содержание ПДн в информационной системе ПДн и (или) в результате которых уничтожаются материальные носители ПДн.

7.4. Уничтожение ПДн, в зависимости в том числе от способа осуществления их обработки и вида материального носителя, содержащего персональные данные, может осуществляться ООО "Микроолап текнолоджис" одним из следующих способов:

- путём удаления ПДн, исключающего возможность их последующего восстановления и осуществляемого в том числе из систем резервного копирования, с использованием средств операционной системы либо с применением специализированного прикладного программного обеспечения;

- с применением программного удаления содержимого путём форматирования;

- уничтожения бумажного носителя ПДн путём измельчения на мелкие части с использованием специального технического оборудования или сжигания;

- уничтожения машинного носителя ПДн путём нанесения неустранимого физического повреждения (включая деформирование, нарушение единой целостности машинного носителя, сжигания).

7.5. Подтверждением уничтожения ООО "Микроолап текнолоджис" ПДн в случаях, предусмотренных законодательством в области ПДн, является акт об уничтожении ПДн и выгрузка из журнала регистрации событий в информационной системе ПДн (при автоматизированной и смешанной обработке ПДн).

8. Порядок и условия обработки персональных данных

8.1. ООО "Микроолап текнолоджис" до начала деятельности по обработке ПДн направляет в уполномоченный орган по защите прав субъектов ПДн (Роскомнадзор) уведомление о намерении осуществлять обработку ПДн с указанием всех необходимых в соответствии с законодательством в области ПДн сведений.

8.2. Сведения о включении ООО «Микроолап текнолоджис» в Реестр операторов, осуществляющих обработку персональных данных, после регистрации будут доступны на сайте Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций в сети «Интернет» по адресу: https://pd.rkn.gov.ru/operators-registry/operators-list/ по номеру записи ООО «Микроолап текнолоджис».

8.3. В случае изменения сведений, указанных ООО "Микроолап текнолоджис" в направленном в уполномоченный орган по защите прав субъектов ПДн уведомлении о намерении осуществлять обработку ПДн, а также в случае прекращения обработки ПДн, ООО "Микроолап текнолоджис" уведомляет об этом уполномоченный орган по защите прав субъектов ПДн в установленные законодательством в области ПДн сроки.

8.4. При организации и осуществлении обработки ПДн ООО "Микроолап текнолоджис" принимает необходимые и достаточные меры по обеспечению выполнения обязанностей, предусмотренных законодательством в области обработки ПДн.

8.5. В ООО "Микроолап текнолоджис" принимаются обязательные для исполнения всеми работниками, а также контрагентами и прочими третьими лицами в части, касающейся передачи и последующей обработки ими ПДн, внутренние нормативные документы, которыми определены, в частности:

- Политика в отношении обработки ПДн;

- назначение лица, ответственного за обработку ПДн, которое осуществляет организацию обработки ПДн, обучение и инструктаж, внутренний контроль за соблюдением Обществом и его работниками требований к защите ПДн.

- установление правил доступа к ПДн, обрабатываемым в ИСПДн ООО "Микроолап текнолоджис", а также обеспечение регистрации и учёта всех действий, совершаемых с ПДн в ИСПДн ООО "Микроолап текнолоджис";

- для каждой цели обработки категории и перечень обрабатываемых ПДн, способы и сроки их обработки, а также категории субъектов ПДн;

- правила и процедура предоставления доступа к ПДн, а также перечень лиц (должностей), которым для выполнения трудовых (должностных) обязанностей необходим доступ к ПДн;

- порядок и правила уничтожения ПДн при достижении целей их обработки или при наступления иных законных оснований;

- процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;

- порядок и правила рассмотрения обращений (запросов) субъектов ПДн (их представителей);

- порядок и правила обработки ПДн без использования средств автоматизации;

- установление индивидуальных паролей доступа сотрудников в информационную систему в соответствии с их производственными обязанностями;

- применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

- сертифицированное антивирусное программное обеспечение с регулярно обновляемыми базами;

- соблюдение условий, обеспечивающих сохранность ПДн и исключающих несанкционированный к ним доступ;

- обнаружение фактов несанкционированного доступа к ПДн и принятие мер;

- восстановление ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

- осуществление внутреннего контроля и аудита.

8.6. В ООО "Микроолап текнолоджис" осуществляется внутренний контроль и (или) аудит соответствия обработки ПДн требованиям законодательства в области ПДн, требованиям к защите ПДн, а также настоящей Политике и иным внутренним нормативным документам ООО "Микроолап текнолоджис".

8.7. ООО "Микроолап текнолоджис" принимает необходимые меры для поддержания точности, достаточности, а в необходимых случаях актуальности ПДн по отношению к целям их обработки.

8.8. ООО "Микроолап текнолоджис" в порядке и в соответствии с требованиями, установленными законодательством в области ПДн, проводит оценку вреда, который может быть причинен субъектам ПДн в случае нарушения Федерального закона от 27.07.2006 г. No 152-ФЗ «О ПДн», а также устанавливает соотношение указанного вреда и принимаемых мер, направленных на обеспечение выполнения обязанностей в соответствии с законодательством в области ПДн.

8.9. Работники ООО "Микроолап текнолоджис", непосредственно осуществляющие обработку ПДн, проходят ознакомление с положениями законодательства о ПДн, в том числе с требованиями к защите ПДн, внутренними нормативными документами по вопросам обработки ПДн, включая определяющие политику ООО "Микроолап текнолоджис" в отношении обработки ПДн.

8.10. Работники ООО "Микроолап текнолоджис", непосредственно осуществляющие обработку ПДн, систематически проходят обучение по вопросам обработки ПДн, положениям законодательства РФ о ПДн, в том числе требованиям к защите ПДн, документам, определяющим политику ООО "Микроолап текнолоджис" в отношении обработки ПДн, локальным актам по вопросам обработки ПДн.

8.11. В ООО "Микроолап текнолоджис" разрабатывается и поддерживается в актуальном состоянии Реестр процессов обработки ПДн.

8.12. ООО "Микроолап текнолоджис" не раскрывает и не распространяет обрабатываемые ПДн третьим лицам.

8.13. ООО "Микроолап текнолоджис" не может передавать, а также поручать обработку ПДн другому (третьему) лицу, если иное не предусмотрено законодательством Российской Федерации.

8.14. ООО "Микроолап текнолоджис" не осуществляет передачу обрабатываемых ПДн на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу (трансграничную передачу ПДн) и не поручает обработку ПДн иностранным лицам.

9. Конфиденциальность и безопасность персональных данных

ПДн сотрудников относятся к конфиденциальной информации ограниченного доступа.

9.1. При обработке ПДн ООО "Микроолап текнолоджис" обеспечивает конфиденциальность и безопасность ПДн, принимая необходимые правовые, организационные и технические меры для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения и других несанкционированных действий в отношении ПДн, в том числе:

- проведение систематической оценки угроз безопасности ПДн при их обработке в ИСПДн и разработка мер и мероприятий по защите ПДн;
- определение необходимого уровня защищенности ПДн, обрабатываемых в ИСПДн, в соответствии с Постановлением Правительства РФ от 01.11.2012 г. No1119 «Об утверждении требований к защите ПДн при их обработке в информационных системах ПДн»;
- применение необходимых для выполнения требований к защите ПДн организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн, исполнение которых обеспечивает определённые уровни защищенности ПДн;
- применение средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия;
- проведение оценки эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию ИСПДн и совершенствование системы защиты ПДн;
- ведение учёта машинных носителей ПДн;
- установление правил и разграничение доступа к ИСПДн, материальным носителям (документам), съёмным (машинным) носителям ПДн;
- обеспечение регистрации и учёта всех действий пользователей и администраторов ИСПДн с ПДн, программными средствами информационных систем, съёмными (машинными) носителями ПДн и средствами защиты информации;
- исключение возможности бесконтрольного прохода в офисы ООО "Микроолап текнолоджис", а также в помещения, где размещены технические средства, с использованием которых осуществляется обработка ПДн, а также помещения, в которых хранятся материальные носители ПДн;
- предотвращение внедрения в информационные системы вредоносных программ;
- предотвращение воздействия на технические средства, с использованием которых осуществляется обработка ПДн, в результате которого нарушается их функционирование;
- использование защищённых каналов связи;
- резервирование и восстановление работоспособности технических средств и программного обеспечения, баз данных и средств защиты информационных систем ПДн;
- выявление инцидентов, связанных с нарушением безопасности ПДн, в том числе обнаружение фактов несанкционированного доступа к ПДн и неправомерной передачи (предоставления, распространения, доступа) ПДн в результате компьютерных атак на информационные системы ПДн;
- принятие мер по обнаружению, предупреждению и ликвидации последствий инцидентов, связанных с нарушением безопасности ПДн, в том числе компьютерных атак на информационные системы ПДн и компьютерные инциденты в них;
- восстановление ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

- повышение уровня знаний работников ООО "Микроолап текнолоджис"в сфере обработки и защиты ПДн;

- регулярное исследование условий и факторов, создающих угрозы безопасности ПДн при их обработке в ИСПДн;

- осуществление контроля за принимаемыми мерами по обеспечению безопасности ПДн и уровнем защищенности информационных систем ПДн, включая проведение внутренних и внешних проверок (аудита) соответствия безопасности ПДн требованиям законодательства в области ПДн, настоящей Политики, иных внутренних документов;

- непрерывное развитие и совершенствование системы информационной безопасности.

9.2. В соответствии с требованиями нормативных правовых документов ООО "Микроолап текнолоджис" создана система защиты ПДн (далее СЗПДн). СЗПДн состоит из подсистем правовой, организационной и технической защиты:

Подсистема правовой защиты представляет собой комплекс правовых, организационно-распорядительных и нормативных документов, обеспечивающих создание, функционирование и совершенствование СЗПДн.

Подсистема организационной защиты включает в себя организацию структуры управления СЗПДн, разрешительной системы, защиты информации при работе с сотрудниками, партнёрами и сторонними лицами. Подсистема включает в себя ряд компонентов и мероприятий, направленных на обеспечение безопасности информации и защиту активов организации.

Подсистема технической защиты включает в себя комплекс технических, программных, программно-аппаратных средств, обеспечивающих защиту ПДн.

9.3. При обработке ПДн без использования средств автоматизации ООО "Микроолап текнолоджис" принимает дополнительные меры по обеспечению безопасности ПДн:

- обеспечение возможности определения мест хранения ПДн (их материальных носителей) и перечня лиц, осуществляющих обработку персональных данных либо имеющих доступ к ним, в отношении каждой категории персональных данных, в том числе посредством утверждения перечня соответственно мест хранения ПДн (их материальных носителей) и перечня лиц (должностей), осуществляющих не автоматизированную обработку ПДн либо имеющих доступ к таким ПДн (их материальным носителям);

- обеспечение раздельного хранения ПДн (их материальных носителей), обработка которых осуществляется в различных целях, несовместимых между собой;

- обеспечение эффективной реализации мер по обеспечению сохранности ПДн (их материальных носителей) и исключения несанкционированного доступ к ним, в том числе посредством определения лиц, ответственных за соблюдения условий обеспечения сохранности ПДн (их материальных носителей) и исключения несанкционированного доступ к ним.

9.4. ООО "Микроолап текнолоджис"обеспечивает взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и в случае обнаружения компьютерного инцидента, повлёкшего неправомерную передачу (предоставление, распространение, доступ) ПДн осуществляет информирование федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности, о таком инциденте в порядке и сроки, установленные законодательством в области ПДн.

10. Права субъектов персональных данных и способы их реализации

10.1.Сотрудник имеет право на получение сведений об Операторе, о месте его нахождения, о наличии у Оператора ПДн, относящихся к конкретному субъекту ПДн, а также на ознакомление с

такими ПДн, за исключением случаев, предусмотренных частью 8 статьи 14 Закона 152-ФЗ «О персональных данных».

10.2. Сотрудник имеет право на получение от Оператора при личном обращении к нему либо при получении Оператором письменного запроса от Сотрудника следующей информации, касающейся обработки его персональных данных, в том числе содержащей:

- порядок обращения к ООО "Микроолап текнолоджис" и направление ему запросов;
- порядок обжалования действий или бездействия ООО "Микроолап текнолоджис";
- подтверждение факта обработки ПДн Оператором, а также цель такой обработки;
- правовые основания и цели обработки ПДн;
- цели и применяемые Оператором способы обработки ПДн;
- наименование и место нахождения Оператора, сведения о лицах (за исключением работников Оператора), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с Оператором или на основании Федерального закона;
- обрабатываемые ПДн, относящиеся к соответствующему субъекту ПДн, источник их получения, если иной порядок предоставления таких данных не предусмотрен Федеральным законом;
- сроки обработки ПДн, в том числе сроки их хранения;
- порядок осуществления субъектом ПДн прав, предусмотренных Федеральным законом;
- информацию об осуществлённой или о предполагаемой трансграничной передаче данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению Оператора, если обработка поручена или будет поручена такому лицу;
- иные сведения, предусмотренные Федеральным законом или другими федеральными законами;
- требовать изменения, уточнения, уничтожения информации о самом себе;
- обжаловать неправомерные действия или бездействие по обработке ПДн и требовать соответствующей компенсации в суде;
- на дополнение ПДн оценочного характера заявлением, выражающим его собственную точку зрения;
- определять представителей для защиты своих ПДн;
- требовать от Оператора уведомления обо всех произведённых в них изменениях или исключениях из них.

10.3. Сотрудник имеет право обжаловать в уполномоченном органе по защите прав субъектов ПДн или в судебном порядке действия или бездействие Оператора, если считает, что последний осуществляет обработку его ПДн с нарушением требований Закона 152-ФЗ «О персональных данных» или иным образом нарушает его права и свободы.

10.4. Сотрудник ПДн имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

10.5. В отношении обработки ПДн, организуемой и осуществляемой ООО "Микроолап текнолоджис", субъекты ПДн имеют следующие права:

– свободно, своей волей и в своём интересе предоставлять согласие на обработку ПДн;

– получать информацию, касающуюся обработки их ПДн, включая доступ к своим ПДн, в порядке, форме и сроки, установленные законодательством в области ПДн;

– требовать уточнения своих ПДн, их блокирования или уничтожения в случае, если такие ПДн являются неполными, устаревшими, неточными, незаконно полученными, не являются необходимыми для заявленной цели обработки;

– отозвать своё согласие на обработку ПДн;

– требовать прекращения обработки ПДн в целях продвижения товаров, работ, услуг на рынке путём осуществления прямых контактов с потенциальным потребителем с помощью средств связи;

– принимать предусмотренные действующим законодательством меры по защите своих прав;

– иные права, предусмотренные законодательством в области ПДн.

10.6. Для реализации своих прав субъект ПДн и иное лицо, действующее в интересах субъектов ПДн, может направить ООО "Микроолап текнолоджис" обращение (запрос), в том числе одним из следующих способов:

– по адресу: 142432, Московская область, Ногинский район, г. Черноголовка, Первый проезд, д.4, оф.317;

– на электронную почту: formal@microolap.ru.

10.7. Обращение (запрос) субъекта ПДн может быть направлено лично либо через представителя.

10.8. Обращение (запрос) субъекта ПДн может быть направлено в любой форме с соблюдением требований действующего законодательства, включая требования к содержанию обращений (запросов) субъектов ПДн.

10.9. ООО "Микроолап текнолоджис" рассматривает поступившее обращение (запрос) субъекта ПДн и направляет субъекту ПДн ответ в сроки, установленные законодательством в области ПДн.

10.10. Ответ на обращение (запрос) субъекта ПДн направляется в той же форме, в которой было получено соответствующее обращение (запрос), либо, при наличии у ООО "Микроолап текнолоджис" объективной возможности, в форме, указанной в соответствующем обращении (запросе) субъекта ПДн.

11. Обязанности ООО "Микроолап текнолоджис".

11.1. ООО "Микроолап текнолоджис" обязан:

- при сборе ПДн предоставить информацию об обработке ПДн субъекту ПДн;
- в случаях если ПДн были получены не от субъекта ПДн, уведомить субъекта;
- при отказе в предоставлении ПДн субъекту разъясняются последствия такого отказа;
- опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки ПДн, к сведениям о реализуемых требованиях к защите ПДн;
- принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн;
- давать ответы на запросы и обращения субъектов ПДн, их представителей и уполномоченного органа по защите прав субъектов ПДн;

Оператор не имеет права:

- собирать и обрабатывать ПДн сотрудников о его расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, частной жизни, за исключением случаев, предусмотренных действующим законодательством;
- получать и обрабатывать ПДн сотрудников о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных Федеральным законом.

11.2. По факту личного обращения либо при получении письменного запроса субъекта ПДн или его представителя Оператор, при наличии оснований, обязан в течение 30 дней с даты обращения

либо получения запроса субъекта ПДн или его представителя предоставить сведения в объёме, установленном Федеральным законом. Такие сведения должны быть предоставлены субъекту ПДн в доступной форме, и в них не должны содержаться ПДн, не относящиеся к другим субъектам ПДн, за исключением случаев, если имеются законные основания для раскрытия таких ПДн.

11.3. Все обращения субъектов ПДн или их представителей регистрируются в Журнале учёта обращений субъектов ПДн по вопросам обработки ПДн.

11.4. В случае отказа в предоставлении субъекту ПДн или его представителю при обращении либо при получении запроса субъекта ПДн или его представителя информации о наличии ПДн о соответствующем субъекте ПДн Оператор обязан дать в письменной форме мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 Закона 152-ФЗ «О персональных данных» или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий 30 дней со дня обращения субъекта ПДн или его представителя, либо с даты получения запроса субъекта ПДн или его представителя.

11.5. В случае получения запроса от уполномоченного органа по защите прав субъектов ПДн о предоставлении информации, необходимой для осуществления деятельности указанного органа, Оператор обязан сообщить такую информацию в уполномоченный орган в течение 30 дней с даты получения такого запроса.

11.6. В случае выявления неправомерной обработки ПДн при обращении или по запросу субъекта ПДн или его представителя либо уполномоченного органа по защите прав субъектов персональных данных Оператор обязан осуществить блокирование неправомерно обрабатываемых ПДн, относящихся к этому субъекту ПДн, с момента такого обращения или получения указанного запроса на период проверки.

11.7. В случае выявления неправомерной обработки ПДн, осуществляемой Оператором, последний в срок, не превышающий трёх рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку ПДн. Об устранении допущенных нарушений Оператор обязан уведомить субъекта ПДн или его представителя, а в случае если обращение субъекта ПДн или его представителя либо запрос уполномоченного органа по защите прав субъектов ПДн были направлены уполномоченным органом по защите прав субъектов ПДн, также указанный орган.

11.8. Субъект ПДн вправе обратиться с требованием прекратить передачу (распространение, предоставление, доступ) своих ПДн, ранее разрешённых субъектом ПДн для распространения, к любому лицу, обрабатывающему его ПДн, в случае несоблюдения положений настоящего пункта или обратиться с таким требованием в суд. Данное лицо обязано прекратить передачу (распространение, предоставление, доступ) ПДн в течение трёх рабочих дней с момента получения требования субъекта ПДн или в срок, указанный во вступившем в законную силу решении суда, а если такой срок в решении суда не указан, то в течение трёх рабочих дней с момента вступления решения суда в законную силу.

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

11.10. В случае достижения цели обработки ПДн Оператор обязан прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий 30 рабочих дней с даты достижения цели обработки ПДн, если иное не предусмотрено согласием на обработку ПДн, стороной которого является субъект ПДн.

11.11. Режим конфиденциальности ПДн.

11.11.1. Оператор обеспечивает конфиденциальность и безопасность ПДн при их обработке в соответствии с требованиями законодательства РФ.

11.11.2. Оператор не раскрывает третьим лицам и не распространяет ПДн без согласия на это субъекта ПДн, если иное не предусмотрено Федеральным законом.

11.11.3. В соответствии с перечнем ПДн, обрабатываемых в ИСПДн ПДн сотрудников являются конфиденциальной информацией.

11.11.4. Лица, осуществляющие обработку ПДн, обязаны соблюдать требования регламентирующих документов Оператора в части обеспечения конфиденциальности и безопасности ПДн.

12. Обработка персональных данных

12.1. Перечень обрабатываемых ПДн пользователей указывает субъект ПДн в согласии на обработку ПДн, разрешённых субъектом ПДн для распространения.

12.2. Лица, имеющие право доступа к ПДн.

12.2.1. Правом доступа к ПДн субъектов обладают лица, наделённые соответствующими полномочиями в соответствии со своими служебными обязанностями.

12.2.2. Перечень лиц, имеющих доступ к персональным данным, утверждается руководителем Оператора.

12.3. Порядок и сроки хранения персональных данных.

12.3.1. Оператор осуществляет только хранение ПДн Пользователей в ИСПДн Оператора.

12.3.2. Сроки хранения ПДн определены условиями Пользовательского соглашения, вводятся в действие с момента принятия (акцепта) Пользователем данного соглашения и действуют до тех пор, пока Пользователь не заявит о своём желании удалить свои ПДн из ИСПДн Оператора.

12.3.3. В случае удаления данных с ИСПДн Пользователя Оператора по инициативе одной из сторон, а именно прекращения использования ИСПДн Оператора, ПДн Пользователей хранятся в базах данных Оператора пять лет в соответствии с законодательством РФ.

12.3.4. По истечении вышеуказанного срока хранения ПДн Пользователей ПДн Пользователей удаляются автоматически заданным алгоритмом, который задаёт Оператор.

12.4. Блокирование персональных данных.

12.4.1. Под блокированием ПДн понимается временное прекращение Оператором операций по их обработке по требованию субъекта при выявлении им недостоверности обрабатываемых сведений или неправомерных, по мнению субъекта ПДн, действий в отношении его данных.

12.4.2. Оператор не передаёт ПДн третьим лицам и не поручает обработку ПДн сторонним лицам и организациям. ПДн субъектов ИСПДн обрабатывают только сотрудники Оператора (администраторы баз данных и т. д.), допущенные установленным порядком к обработке ПДн Пользователей.

12.4.3. Блокирование ПДн на Сайте осуществляется на основании письменного заявления от субъекта ПДн.

12.5. Уничтожение ПДн.

12.5.1. Под уничтожением ПДн понимаются действия, в результате которых становится невозможным восстановить содержание ПДн ИСПДн оператора и/или в результате которых уничтожаются материальные носители ПДн.

12.5.2. Субъект ПДн вправе в письменной форме требовать уничтожения своих ПДн в случае, если ПДн являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки.

12.5.3. В случае отсутствия возможности уничтожения ПДн Оператор осуществляет блокирование таких ПДн.

12.5.4. Уничтожение ПДн осуществляется путём стирания информации с использованием сертифицированного программного обеспечения с гарантированным уничтожением (в

соответствии с заданными характеристиками для установленного программного обеспечения с гарантированным уничтожением).

13. Заключительные положения

13.1. Настоящая Политика вступает в силу с момента её утверждения и действует бессрочно до принятия новой Политики.

Политика вводится в действие в порядке, установленном внутренними нормативными документами ООО "Микроолап текнолоджис", и подлежит обязательному опубликованию на официальном сайте ООО "Микроолап текнолоджис" в ИТК сети «Интернет», размещённом по адресу: https://www.microolap.ru/privacy/, в установленные распорядительным документом ООО "Микроолап текнолоджис" сроки.

13.2. ООО "Микроолап текнолоджис" вправе в одностороннем порядке пересматривать либо вносить изменения в настоящую Политику, в частности, для актуализации каких-либо установленных ей правил и требований, а также в случае необходимости приведения её в соответствие с требованиями действующего законодательства в области ПДн.

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

13.4. Настоящая Политика обязательна для ознакомления под подпись и исполнения всеми работниками ООО "Микроолап текнолоджис", осуществляющими обработку и (или) защиту ПДн либо иным образом участвующими в сопряжённых с обработкой и (или) защитой ПДн процессах.

13.5. Контроль исполнения требований настоящей Политики при организации и осуществлении обработки и защиты ПДн ООО "Микроолап текнолоджис" осуществляют ответственный за организацию обработки ПДн и ответственный за обеспечение безопасности ПДн.

13.5. В случае нарушения требований настоящей Политики, в том числе в случае нарушения конфиденциальности и (или) безопасности ПДн, работники могут быть привлечены к дисциплинарной, материальной, гражданско-правовой, административной и уголовной ответственности в соответствии с законодательством Российской Федерации.

13.6. Все изменения и дополнения к настоящей Политике утверждаются генеральным директором ООО «Микроолап текнолоджис».

13.7. Ответственность за нарушение требований правовых нормативных документов Российской Федерации и нормативных документов ООО «Микроолап текнолоджис» в области ПДн определяется в соответствии с законодательством Российской Федерации.

13.7.1. Все сотрудники Оператора, осуществляющие обработку ПДн, обязаны хранить тайну о сведениях, содержащих персональные данные, в соответствии с Положением, требованиями законодательства РФ.

13.7.2. Лица, виновные в нарушении требований Положения, несут предусмотренную законодательством РФ ответственность.

13.7.3. Ответственность за соблюдение режима ПДн по отношению к ПДн, находящимся в базах данных Сайта, несут ответственные за обработку ПДн.

13.8. В случае изменения действующего законодательства РФ, внесения изменений в нормативные документы по защите ПДн настоящее Положение действует в части, не противоречащей действующему законодательству до приведения его в соответствие с такими.

Приложение 1. Основные понятия, термины и определения.

Приложение 2. Нормативные правовые акты обработки и защиты персональных данных.

Ответственный за обработку персональный данных

Приложение 1
к Политике обработки персональных данных

Основные понятия, термины и определения

Автоматизированная обработка персональных данных – обработка ПДн с помощью средств вычислительной техники.

Актуальные угрозы безопасности персональных данных - совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к ПДн при их обработке в информационной системе (далее ИС), результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение ПДн, а также иные неправомерные действия.

Блокирование персональных данных – временное прекращение обработки ПДн (за исключением случаев, если обработка необходима для уточнения ПДн).

Информационная система персональных данных (ИСПДн) – совокупность содержащихся в базах данных ПДн и обеспечивающих их обработку информационных технологий и технических средств.

ИСПДн сотрудников оператора, если в информационной системе обрабатываются ПДн только указанных сотрудников.

ИСПДн общедоступных персональных данных - ИСПДн, если в информационной системе обрабатываются ПДн субъектов персональных данных, полученные только из общедоступных источников персональных данных, созданных в соответствии со статьей 8 Федерального закона "О персональных данных".

Защита персональных данных – деятельность, направленная на предотвращение утечки защищаемых ПДн, несанкционированных и непреднамеренных воздействий на защищаемые ПДн.

Мониторинг и аудит: Системы, отслеживающие доступ к данным и действия пользователей, что позволяет выявлять и предотвращать несанкционированные действия.

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

Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность ПДн конкретному субъекту ПДн.

Оператор – государственный орган, муниципальный орган, *юридическое* или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие *обработку ПДн, а также определяющие цели обработки ПДн, состав ПДн, подлежащих обработке, действия (операции), совершаемые с ПДн*.

Персональные данные (**ПДн**) – любая информация, относящаяся к прямо или косвенно определённому или определяемому физическому лицу (**субъекту ПДн**).

Персональные данные, разрешённые субъектом ПДн для распространения, – это ПДн, доступ неограниченного круга лиц к которым предоставлен субъектом ПДн путём дачи согласия на обработку ПДн, разрешённых субъектом ПДн для распространения.

Предоставление персональных данных – действия, направленные на раскрытие ПДн определённому лицу или определённому кругу лиц.

Пользователь – пользователь сети Интернет и, в частности, Сайтов информационных сервисов обработки ПДн ООО «Микроолап текнолоджис» и операторов ПДн сторонних организаций, имеющий свой профиль/аккаунт.

Распространение персональные данные – действия, направленные на раскрытие ПДн неопределённому кругу лиц.

Сайт – совокупность программных и аппаратных средств для ЭВМ, обеспечивающих публикацию информации и данных, объединённых общим целевым назначением, посредством технических средств, применяемых для связи между ЭВМ в сети Интернет.

Под **Сайтом** в настоящей Политике понимаются в зависимости от цели обрабатываемой информации сайты использования информационных сервисов обработки ПДн ООО «Микроолап текнолоджис» и сторонних операторов ПДн, расположенных в сети Интернет по адресу:

http://www.microolap.ru - официальный сайт компании ООО Микроолап текнолоджис»;

http://kedo.kontur.ru - ИСПДн кадрового электронного документа оборота «Контур.КЭДО» АО "ПФ "СКБ КОНТУР" для обмена кадровыми документами между работодателем и сотрудниками ООО Микроолап текнолоджис»;

http://diadoc.kontur.ru - ИСПДн электронного документа оборота «Контур.Диадок» АО "ПФ "СКБ КОНТУР" для обмена электронными документами между ООО Микроолап текнолоджис» и контрагентами;

http://btrx.l7.cx - Программный комплекс «1С-Битрикс24» от компании ООО «Битрикс» для ведения электронного документа оборота ООО «Микроолап текнолоджис»;

http://tbank.ru - ИСПДн банка АО «ТБанк» для учёта зарплаты, подготовки отчётных сведений ООО «Микроолап текнолоджис» для ФНС и СФР.

Трансграничная передача персональных данных – передача ПДн на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

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

Приложение 2
к Политике обработки персональных данных

Нормативные правовые акты обработки и защиты ПДн

*Законодательство Российской Федерации основывается на **Конституции Российской Федерации** и международных договорах Российской Федерации. Правовая основа организации работы в области информационной безопасности (ИБ) включает в себя федеральные законы (ФЗ), подзаконные акты, международные стандарты, нормативные акты, правовые акты (далее - нормативные правовые акты), внутренние регламенты и политики компании. Соблюдение этих норм и требований является необходимым условием для эффективной защиты информации (далее ЗИ) и минимизации рисков, связанных с её обработкой и хранением; базируется на ряде нормативных актов и стандартов, регулирующих вопросы ЗИ.*

http://publication.pravo.gov.ru/ - Официальное опубликование правовых актов.

https://fstec.ru/ - ФСТЭК, Федеральный орган исполнительной власти, осуществляющий реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности.

http://www.fsb.ru/ ФСБ России, Федеральная служба безопасности Российской Федерации.

https://rkn.gov.ru/ - Роскомнадзор, Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций.

https://rostest.info/nashi-kontakty/ - Центр сертификации «Ростест Инфо».

Конституция Российской Федерации

Принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020.

ФЕДЕРАЛЬНЫЕ ЗАКОНЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

Закон РФ от 21.07.1993 N 5485-1 "О государственной тайне"

Закон регулирует отношения, связанные с отнесением сведений к государственной тайне, их засекречиванием или рассекречиванием и защитой государственной тайны в интересах обеспечения безопасности Российской Федерации. Основные понятия, используемые в настоящем Законе...

Федеральный закон № 152-ФЗ «О персональных данных» от 27 июля 2006 года.

Закон определяет порядок сбора, хранения, использования и защиты персональных данных граждан. Он обязывает операторов персональных данных принимать меры для защиты этих данных от несанкционированного доступа, изменения, уничтожения или распространения.

Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации".

Закон регулирует отношения, возникающие при создании, обработке, распространении и защите информации, а также устанавливает принципы обеспечения информационной безопасности.

Федеральный закон от 19.12.2005 N 160-ФЗ "О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных".

Российская Федерация заявляет, что в соответствии с подпунктом "a" пункта 2 статьи 9 Конвенции оставляет за собой право устанавливать ограничения права субъекта персональных данных на доступ к персональным данным о себе в целях защиты безопасности государства и общественного порядка.

Федеральный закон от от 30.12.2001 N 197-ФЗ "Трудовой кодекс Российской Федерации" Закреплены положения:

- *Общие требования при обработке персональных данных работника и гарантии их защиты;*
- *Хранение и использование персональных данных работников;*
- *Передача персональных данных работника;*
- *Права работников в целях обеспечения защиты персональных данных, хранящихся у работодателя;*
- *Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных работника.*

Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 N 195-ФЗ.

Статья 13.11. Нарушение законодательства РФ в области персональных данных - устанавливает ответственность в виде наложения административного штрафа на граждан, должностных лиц и. на юридических лиц.

Указ Президента РФ от 6 марта 1997 года № 188 "Об утверждении Перечня сведений конфиденциального характера «О утверждении перечня сведений конфиденциального характера».

Утверждён прилагаемый Перечень сведений конфиденциального характера (частной жизни гражданина, Сведения, составляющие тайну следствия и судопроизводства и т.д.).

Указ Президента РФ от 01.05.2022 N 250 "О дополнительных мерах по обеспечению информационной безопасности Российской Федерации"

Реализация дополнительных организационных и технических мер по обеспечению информационной безопасности организации, в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты.

ПОДЗАКОННЫЕ АКТЫ

ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

Постановление Правительства Российской Федерации от 15.09.2008 N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации"

Правила обработки персональных данных, осуществляемой без использования средств автоматизации, установленные нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами организации, должны применяться с учётом требований настоящего Положения."

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

Документ устанавливает требования к защите персональных данных при их обработке в информационных системах персональных данных (далее - информационные системы) и уровни защищенности таких данных.

Система защиты персональных данных включает в себя организационные и (или) технические меры, определённые с учётом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах.

Постановление Правительства Российской Федерации от 29.06.2021 N 1046 "О федеральном государственном контроле (надзоре) за обработкой персональных данных" (вместе с "Положением о федеральном государственном контроле (надзоре) за обработкой персональных данных").

Положение устанавливает порядок организации и осуществления федерального государственного контроля (надзора) за обработкой персональных данных.

Постановление Правительства Российской Федерации от 03.02.2012 N 79 "О лицензировании деятельности по технической защите конфиденциальной информации" (вместе с "Положением о лицензировании деятельности по технической защите конфиденциальной информации")

Определяет порядок лицензирования деятельности по технической защите конфиденциальной информации (не содержащей сведения, составляющие государственную тайну, но защищаемой в соответствии с законодательством Российской Федерации).. Содержит перечень лицензионных требований и условий для производства СЗИ, включая криптографические средства.

Постановление Правительства Российской Федерации от 23.03.2024 N 367 "О внесении изменений в некоторые акты Правительства Российской Федерации", в части изменения Положения о единой системе межведомственного электронного взаимодействия:

- федеральной государственной информационной системе "Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме";

- единой информационной системы персональных данных (единой биометрической системы), обеспечивающей обработку, включая сбор и хранение биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным физического лица заменить словами.

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО НАДЗОРУ В СФЕРЕ СВЯЗИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И МАССОВЫХ КОММУНИКАЦИЙ, РОСКОМНАДЗОР

Роскомнадзор (РКН). Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 24.02.2021 № 18 "Об утверждении требований к содержанию согласия на обработку персональных данных, разрешённых субъектом персональных данных для распространения".

Документ устанавливает требования к содержанию согласия на обработку персональных данных, разрешённых субъектом персональных данных для распространения.

Роскомнадзор (РКН). Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 21 июня 2021 г. № 106 "Об утверждении Правил использования информационной системы Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций, в том числе порядка взаимодействия субъекта персональных данных с оператором"

Правила устанавливают порядок использования информационной системы Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций, в том числе порядок взаимодействия субъекта персональных данных с оператором, для обеспечения получения оператором согласия на обработку персональных данных, разрешённых субъектом персональных данных для распространения.

Роскомнадзор (РКН). Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 27.10.2022 № 178 "Об утверждении Требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона "О персональных данных".

Оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных" осуществляется ответственным за организацию обработки персональных данных либо комиссией, образуемой оператором.

Роскомнадзор (РКН). Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 28.10.2022 от 10 июля 2014 года 179 "Об утверждении Требований к подтверждению уничтожения персональных данных".

Документ устанавливает требования к документам, если обработка персональных данных осуществляется оператором без использования средств автоматизации и с использованием средств автоматизации.

Роскомнадзор (сокращённо РКН). Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 28.10.2022 № 180 "Об утверждении форм уведомлений о намерении осуществлять обработку персональных данных, об изменении сведений, содержащихся в уведомлении о намерении осуществлять обработку персональных данных, о прекращении обработки персональных данных".

Формы Уведомлений о намерении осуществлять обработку персональных данных, о прекращении обработки персональных данных"

Роскомнадзор (РКН). Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 14.11.2022 N 187 "Об утверждении

Порядка и условий взаимодействия Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций с операторами в рамках ведения реестра учёта инцидентов в области персональных данных"

Порядок и условия Взаимодействие Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций с операторами в целях учёта в реестре учёта инцидентов в области персональных данных информации о факте неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлёкшей нарушение прав субъектов персональных данных, осуществляется в форме направления операторами в Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций уведомления о таких фактах (далее — уведомление).

Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 24.02.2021 N 18 "Об утверждении требований к содержанию согласия на обработку персональных данных, разрешённых субъектом персональных данных для распространения".

Требования к содержанию согласия на обработку персональных данных, разрешённых субъектом персональных данных для распространения.

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ РОССИЙСКОЙ ФЕДЕРАЦИИ, ФСТЭК

УТВЕРЖДЕН директором ФСТЭК России 12 августа 2020 г.

Перечень технической документации, национальных стандартов и методических документов, *необходимых для выполнения работ и оказания услуг, установленных положением о лицензировании деятельности технической защите конфиденциальной информации*, утвержденным **Постановлением Правительства Российской Федерации от 3 февраля 2012 г. N 79**.

Приказ Федеральной службы по техническому и экспортному контролю от 18.02.2013 N 21 (ред. от 14.05.2020) "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных"

Приказ содержит перечень мер, которые должны приниматься операторами персональных данных для защиты этих данных.

Приказ Федеральной службы по техническому и экспортному контролю от 17.07.2017 N 134 (ред. От 02.12.2020) "Об утверждении Административного регламента Федеральной службы по техническому и экспортному контролю по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации"

Административный регламент предоставления Федеральной службой по техническому и экспортному контролю государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации (далее - Регламент) определяет сроки и последовательность выполнения административных процедур (действий) Федеральной службой по техническому и экспортному контролю при предоставлении государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации (далее -государственная услуга).

Заявителями на получение государственной услуги являются юридические лица и индивидуальные предприниматели, планирующие осуществлять (осуществляющие) деятельность по технической защите конфиденциальной информации (далее - заявитель, соискатель лицензии,лицензиат).

Приказ Федеральной службы по техническому и экспортному контролю от 11.02.2013 N 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах"

В документе устанавливаются требования к обеспечению защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну (далее - информация), от утечки по техническим каналам, несанкционированного доступа, специальных воздействий на такую информацию (носители информации) в целях ее добывания, уничтожения, искажения или блокирования доступа к ней (далее - защита информации) при обработке указанной информации в государственных информационных системах.

утв. Гостехкомиссией РФ 25.11.1994 - «Положение по аттестации объектов информатизации по требованиям безопасности информации».

Положение устанавливает основные принципы, организационную структуру системы аттестации объектов информатизации по требованиям безопасности информации, порядок проведения аттестации, а также контроля и надзора за аттестацией и эксплуатацией аттестованных объектов информатизации.

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ, ФСБ РОССИИ

ФАПСИ. ПРИКАЗ Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13 июня 2001 г. N 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»

ФСБ. Утверждены руководством 8 Центра ФСБ России 21 февраля 2008 г. N 149/6/6-622 «ТИПОВЫЕ ТРЕБОВАНИЯ ПО ОРГАНИЗАЦИИ И ОБЕСПЕЧЕНИЮ ФУНКЦИОНИРОВАНИЯ ШИФРОВАЛЬНЫХ (КРИПТОГРАФИЧЕСКИХ) СРЕДСТВ, ПРЕДНАЗНАЧЕННЫХ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ, НЕ СОДЕРЖАЩЕЙ СВЕДЕНИЙ, СОСТАВЛЯЮЩИХ ГОСУДАРСТВЕННУЮ ТАЙНУ, В СЛУЧАЕ ИХ ИСПОЛЬЗОВАНИЯ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ.

ФСБ. ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ ПРИКАЗ от 9 февраля 2005 г. N 66 «ОБ УТВЕРЖДЕНИИ ПОЛОЖЕНИЯ О РАЗРАБОТКЕ, ПРОИЗВОДСТВЕ, РЕАЛИЗАЦИИ И ЭКСПЛУАТАЦИИ ШИФРОВАЛЬНЫХ (КРИПТОГРАФИЧЕСКИХ) СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ (ПОЛОЖЕНИЕ ПКЗ-2005)

ФСБ. Приказ Федеральной службы безопасности Российской Федерации от 13.02.2023 N 77 "Об утверждении порядка взаимодействия операторов с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, включая информирование ФСБ России о компьютерных инцидентах, повлёкших неправомерную передачу (предоставление, распространение, доступ) персональных данных".

ФСБ. Приказ Федеральной службы безопасности Российской Федерации № 378 от 10 июля 2014 года «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

Приоритетным является документ, устанавливающий требования к использованию средств криптографической защиты информации. Подробно описывает административные процедуры и требования к получению лицензии на производство СЗИ.

ФСБ. Приказ Федеральной службы по техническому и экспортному контролю от 18.02.2013 N 21 (ред. от 14.05.2020) "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных"

Приказ содержит перечень мер, которые должны приниматься операторами персональных данных для защиты этих данных.

РОСТЕСТ ИНФО

ГОСТ Р 50922-96 «Защита информации. Основные термины и определения»

Стандарт описывает основные понятия и термины, используемые в области информационной безопасности, включая защиту персональных данных.

https://rostest.info/gost/001.001.040.001/gost-r-50922-96/

https://docs.cntd.ru/document/1200004674?ysclid=m6hyofu3zr837173675
https://proffadmin.ru/upload/iblock/0de/gost-r-50922_2006-zashchita-informatsii.pdf

ПРИКАЗ Ростехрегулирования от 27 декабря 2006 г. N 373-ст ОБ УТВЕРЖДЕНИИ НАЦИОНАЛЬНОГО СТАНДАРТА. Утвердить национальный стандарт РФ ГОСТ Р 50922-2006 "Защита информации. Основные термины и определения" с датой введения в действие 1 февраля 2008 г.

ГОСТ Р 51275-2006 "Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения"

Стандарт устанавливает классификацию и перечень факторов, воздействующих на безопасность защищаемой информации, в целях обоснования угроз безопасности информации и требований по защите информации на объекте информатизации.

Стандарт распространяется на объекты информатизации, создаваемые и эксплуатируемые в различных областях деятельности (обороны, экономики, науки и других областях)

ГОСТ Р 51583-2014 "Защита информации. Порядок создания автоматизированных систем в защищённом исполнении. Общие положения"

Определят порядок создания автоматизированных систем, использующих СЗИ.

ГОСТ Р 56939-2024 "Защита информации. Разработка безопасного программного обеспечения. Общие требования" (утв. и введён в действие приказом Федерального агентства по техническому регулированию и метрологии от 24 октября 2024 г. N 1504-ст) Взамен ГОСТ Р 56939-2016. https://base.garant.ru/410749342/

стандарт направлен на достижение целей, связанных с предотвращением появления, выявлением и устранением недостатков, в том числе уязвимостей, в программном обеспечении, и содержит общие требования, предъявляемые к разработчикам и производителям программного обеспечения при реализации процессов разработки безопасного программного обеспечения.

РОССТАНДАРТ

Приказ Росстандарта от 08.12.2016 N 2004-ст (ред. от 14.05.2018) "**ГОСТ Р 7.0.97-2016**. Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Организационно - распорядительная документация. Требования к оформлению документов"

Стандарт распространяется на организационно-распорядительные документы: уставы, положения, правила, инструкции, регламенты, постановления, распоряжения, приказы, решения, протоколы, договоры, акты, письма, справки и др. (далее - документы), в том числе включённые в ОК 011-93 "Общероссийский классификатор управленческой документации" (ОКУД), класс 0200000.

Настоящий стандарт определяет состав реквизитов документов, правила их оформления, в том числе с применением информационных технологий; виды бланков, состав реквизитов бланков, схемы расположения реквизитов на документе; образцы бланков; правила создания документов. Положения настоящего стандарта распространяются на документы на бумажном и электронном носителях.

Приказ Росстандарта от 18.01.2024 N 25-ст"Об утверждении национального стандарта Российской Федерации" **ГОСТ Р 71207-2024** «Защита информации. Разработка безопасного программного обеспечения. Статический анализ программного обеспечения. Общие требования»

Настоящий стандарт устанавливает:

- *устанавливает общие требования к внедрению и выполнению статического анализа ПО, а также исходные данные, необходимые для его выполнения*
- *устанавливает требования к методам статического анализа, инструментам анализа (статическим анализаторам) и к специалистам, участвующим в анализе.*
- *устанавливает методику проверки устанавливаемых требований к инструментам анализа.*
- *входит в комплекс стандартов, направленных на достижение целей, связанных с преотвращением появления и/или устранением уязвимостей программ, содержит общие требования по проведению статического анализа ПО и применяется совместно с ГОСТ Р 56939.*