603089, Нижний Новгород, Сергиевская, 21

ПОЛИТИКА В ОТНОШЕНИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

СОДЕРЖАНИЕ

1.ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Политика по организации обработки персональных данных (далее – Политика) устанавливает требования к обработке персональных данных (далее – ПДн) в процессах ООО «Меритерра» (далее – Компания, Оператор).

Настоящая Политика разработана с учетом требований следующих документов:

- ISO/IEC 27001:2013 «Information technology — Security techniques — Information security management systems — Requirements»;
- ISO/IEC 27701:2019 « Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines»;
- Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных";
- Положение об обработке персональных данных.

Политика распространяется на все структурные подразделения в области действия системы

менеджмента информационной безопасности (СМИБ) Компании.

В Политике используются следующие термины с соответствующими определениями и сокращения:

- оператор персональных данных (оператор) - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;
- обработка персональных данных - любое действие (операция) или совокупность действий (операций) с персональными данными, совершаемых с использованием средств автоматизации или без их использования;
- биометрические ПДн – сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются для установления личности субъекта данных (фотографическое изображение, изображение лица, голос, рисунок сосудов ладони, изображения отпечатков пальцев, рисунок радужки глаза, характеристики поведения при взаимодействии с автоматизированными системами);
- блокирование ПДн – временное прекращение обработки ПДн (кроме хранения);
- обезличивание ПДн – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность ПДн конкретному субъекту данных;
- персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);
- рабочее устройство – средство вычислительной техники, предназначенное для исполнения должностных обязанностей и предоставленное работнику для эксплуатации установленным в Компании порядком;
- специальные категории ПДн – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни;
- трансграничная передача ПДн – передача ПДн на территорию иностранного государства;
- хранение ПДн – процесс поддержания исходного состава ПДн в виде, обеспечивающем выдачу ПДн по запросам конечных пользователей в установленные сроки;
- чек-бокс (от англ. check box) – галочка, крестик, иной символ внутри элемента графического пользовательского интерфейса, проставляемый субъектом данных и позволяющий субъекту данных управлять параметром с двумя состояниями – включено/выключено;
- ИС – информационная система;
- ПДн – персональные данные.

1.2. Основные права и обязанности Оператора.

1.2.1. Оператор имеет право:
1. самостоятельно определять состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Законом о персональных данных и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено Законом о персональных данных или другими федеральными законами;
2. в случае отзыва субъектом персональных данных согласия на обработку персональных данных Оператор вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии оснований, указанных в Законе о персональных данных.
1.2.2. Оператор обязан:
1. организовывать обработку персональных данных в соответствии с требованиями Закона о персональных данных;
2. отвечать на обращения и запросы субъектов персональных данных и их законных представителей в соответствии с требованиями Закона о персональных данных;
3. сообщать в уполномоченный орган по защите прав субъектов персональных данных (Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор)) по запросу этого органа необходимую информацию установленные сроки.
4. в случае достижения цели обработки персональных данных незамедлительно прекратить обработку персональных данных и уничтожить соответствующие персональные данные 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 Компанией и субъектом персональных данных.

1.3. Основные права и обязанности субъекта персональных данных.

1.3.1. Субъект персональных данных имеет право:
1. получать информацию, касающуюся обработки его персональных данных, за исключением случаев, предусмотренных федеральными законами. Сведения предоставляются субъекту персональных данных Оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, когда имеются законные основания для раскрытия таких персональных данных. Перечень информации и порядок ее получения установлен Законом о персональных данных;
2. требовать от оператора 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. Требовать устранения неправомерных действий Компании в отношении его персональных данных.
3. обжаловать действия или бездействие Компании в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.
1.3.2. Субъект персональных данных обязан:
1. сообщать достоверную информацию о себе и предоставлять документы, содержащие персональные данные, состав которых установлен законодательством Российской Федерации и локальными нормативными документами Компании в объеме, необходимом для цели обработки;
2. сообщать в Компанию об уточнении (обновлении, изменении) своих персональных данных.
1.4. Требования настоящей Политики являются обязательными для исполнения всеми работниками Компании, занимающими должности, замещение которых предусматривает осуществление обработки персональных данных.
Обработка ПДн может состоять из следующих действий (операций), совершаемых с ПДн:

- сбор (поступление), запись ПДн;
- систематизация, накопление, хранение, размещение, использование ПДн;
- уточнение (обновление, изменение) ПДн;
- извлечение, передача (предоставление, доступ) ПДн;
- обезличивание, блокирование, удаление, уничтожение ПДн.

2.ПРАВОВЫЕ ОСНОВАНИЯ И ЦЕЛИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.
2.2. Обработке подлежат только персональные данные, которые отвечают целям их обработки.
2.3. Обработка Оператором персональных данных осуществляется в следующих целях: осуществление своей деятельности в соответствии с уставом ООО "Меритерра", в том числе заключение и исполнение договоров с контрагентами; исполнение трудового законодательства в рамках трудовых и иных непосредственно связанных с ним отношений, в том числе: содействие работникам в трудоустройстве, получении образования и продвижении по службе, привлечение и отбор кандидатов на работу у Оператора, обеспечение личной безопасности работников, контроль количества и качества выполняемой работы, обеспечение сохранности имущества, ведение кадрового и бухучета, заполнение и передача в уполномоченные органы требуемых форм отчетности, организация постановки на индивидуальный (персонифицированный) учет работников в системе обязательного пенсионного страхования.

2.4. Компания осуществляет обработку и обеспечивает безопасность персональных данных для осуществления возложенных на Компанию законодательством России функций, полномочий и обязанностей в том числе, но не ограничиваясь, в соответствии с Конституцией Российской Федерации, федеральными законами, в частности Федеральным законом № 152-ФЗ от 27 июля 2006 года "О персональных данных", подзаконных актов, других определяющих случаи и особенности обработки указанных персональных данных федеральных законов Российской Федерации, а также Гражданским кодексом Российской Федерации, Налоговым кодексом Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом № 402-ФЗ от 6 декабря 2011 г. "О бухгалтерском учете", а также уставом и локальными актами Компании, согласием на обработку персональных данных.
2.5. Обработка Оператором биометрических персональных данных осуществляется в соответствии с законодательством Российской Федерации.

3.ТРЕБОВАНИЯ К ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1 Сбор (поступление) ПДн

Источники сбора (поступления) ПДн. Компания может получать ПДн из следующих источников:

- от субъекта данных;
- от иного лица, а именно:

o от иного лица, в случае если субъект данных является (или будет являться) выгодоприобретателем или поручителем по заключенному (или заключаемому) договору между Компанией и иным лицом;

o от партнера Компании по договору-поручения или иному договору, предусматривающему обработку ПДн, в том числе, передачу;

- из общедоступных источников, а именно:

o из публичных источников, в которых ПДн подлежат опубликованию или обязательному раскрытию в соответствии с требованиями законодательства;

o из СМИ;

o из иных источников (социальные сети, площадки продаж и т.д.).

3.2 Условия сбора (поступления) ПДн.

Компания может получать ПДн при соблюдении следующих условий:

- субъект данных дал согласие на обработку своих персональных данных для одной или нескольких конкретных целей;
- обработка нужна для выполнения договора, в котором субъект данных является заключающей договор стороной, или для принятия мер по требованию субъекта данных до заключения договора;

- обработка нужна для защиты жизненных интересов субъекта данных или других лиц;
- обработка нужна для выполнения задач в интересах Компании или при осуществлении оператором ПДн законно предоставленных официальных полномочий;
- обработка необходима для соблюдения законных интересов оператора ПДн или третьего лица, за исключением, если интересы или основные права и свободы субъекта данных, для которых требуется защита персональных данных, являются более важными, чем такого рода интересы, в особенности, если субъектом данных является ребёнок.

Компания не реализует процессы, предусматривающие принятие решений на основании исключительно автоматизированной обработки ПДн, порождающего юридические последствия в отношении субъекта данных или иным образом затрагивающее его права и законные интересы.

3.3 Запись ПДн

Запись ПДн заключается в фиксировании ПДн в базах данных или информационных системах в установленных форматах.
Форматы записи определяются технологическими полями ввода информации в соответствующих ИС.

3.4 Накопление ПДн

Накопление – процесс увеличения исходного массива ПДн, необходимого для выполнения функциональных задач процессов Компании и поддержания ПДн в актуальном состоянии.
Формирование массива ПДн основывается на принципах необходимого содержания, объема и отсутствия избыточности ПДн по отношению к заявленным целям их обработки.
Накопление ПДн осуществляется в электронном виде в структурных подразделениях Компании.

3.5 Хранение ПДн

Хранение ПД может осуществляться следующими способами:

- в электронном виде:
- в ИС Компании;
- на рабочих устройствах.

Хранение ПДн осуществляется в форме, позволяющей определить субъекта данных, но не дольше, чем этого требуют цели обработки ПДн.
Хранение ПДн в электронном виде осуществляется при условии разграничения доступа к ПДн. Хранение ПДн на средствах вычислительной техники осуществляется в течение срока, минимально необходимого для обработки ПДн.

3.6 Использование ПДн

Использование ПДн осуществляется для достижения конкретных, заранее определенных

Компанией целей. На основании определенных целей обработки ПДн и образующихся в процессе такой обработки различных видов документов, устанавливаются сроки обработки ПДн.

3.7 Уточнение (обновление, изменение) ПДн

Уточнение (обновление, изменение) ПДн субъекта данных осуществляется в следующих случаях:

- обращения в Компании субъекта данных об изменении ПДн;
- установления Компанией расхождений в ранее полученных ПДн.

В случае выявления неточных ПДн следует осуществить блокирование персональных данных, относящихся к субъекту, или обеспечить их блокирование, если обработка ПДн осуществляется другим лицом, действующим по поручению Компании.
В случае подтверждения факта неточности ПДн Компания на основании сведений, представленных субъектом данных, обязана уточнить ПДн либо обеспечить их уточнение, если обработка ПДн осуществляется другим лицом, действующим по поручению Компании.
В случае невозможности уточнить ПДн лицо, осуществляющее обработку ПДн по поручению, обязано удалить неточные данные.
Уточнение ПДн и снятие блокирования необходимо произвести в течение 7 (семи) календарных дней со дня получения сведений об их изменении.
Уточнение ПДн в электронном виде производится путем изменения устаревших (не соответствующих действительности) атрибутов ПДн субъекта данных.
В случае уточнения ПДн по заявлению субъекта данных Компания обязана уведомить их о произведенных изменениях ПДн.

3.8 Передача (предоставление) ПДн

Компании может осуществлять передачу ПДн третьим лицам в следующих случаях:

- передача ПДн осуществляется с согласия субъекта данных на передачу его ПДн;
- передача ПДн осуществляется в рамках исполнения договора, стороной которого либо выгодоприобретателем или поручителем, по которому является субъект данных, кроме случаев, требующих наличие согласия субъекта данных;
- передача ПДн осуществляется с согласия субъекта данных при поручении обработки ПДн третьему лицу;
- в иных случаях, предусмотренных применимым законодательством.

Перед осуществлением передачи ПДн третьим лицам подразделением-инициатором проводится проверка наличия правовых оснований на такую передачу.
Передача ПДн третьему лицу осуществляется на основе договора с третьим лицом, предусматривающим такую передачу. В договор рекомендуется включать условия по передаче и защите ПДн, о способе (канале) передачи ПДн или порядке его определения.
Компания, являясь оператором, вправе поручить обработку ПДн другому лицу с согласия

субъекта персональных данных, на основании заключаемого с этим лицом договора (далее – Поручения).
В Поручении в общем случае указываются:

- перечень действий (операций) с ПДн, которые будут совершаться этим лицом;
- цели обработки ПДн;
- обязанность этого лица соблюдать конфиденциальность ПДн и обеспечивать безопасность ПДн при их обработке;
- требования к защите обрабатываемых ПДн;
- порядок информирования передающей стороны об утечке ПДн;
- порядок уничтожения ПДн;
- порядок обработки обращений субъекта данных.

ПДн могут передаваться в электронном виде по электронным каналам связи с использованием средств шифрования (путем шифрования сообщения и/или канала передачи информации) на основании соглашения о неразглашении конфиденциальной информации или соглашения об электронном взаимодействии, заключаемом между сторонами.

3.9 Доступ к ПДн

Доступ к обрабатываемым Компанией ПДн предоставляется только тем работникам Компании, которым он необходим в связи с исполнением ими своих трудовых обязанностей.

3.10. Обезличивание ПДн

Обезличивание ПДн означает совершение действий, в результате которых становится невозможным без использования дополнительной информации определить принадлежность ПДн конкретному субъекту данных.
Компания может без согласия субъектов данных обрабатывать обезличенные данные в статистических или иных исследовательских целях, за исключением использования обезличенных данных в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи.
Допускается обработка обезличенных данных в иных целях, предусмотренных в согласиях субъектов данных.
Обезличивание ПДн не означает их уничтожение и не может использоваться вместо уничтожения ПДн в случаях, установленных законодательством.
Обезличивание ПДн должно обеспечивать не только защиту от несанкционированного использования, но и возможность их дальнейшей обработки.

Обязательные требования при обезличивании ПДн:
1) требования к свойствам обезличенных данных, получаемых при применении метода обезличивания:

- сохранение полноты (состав обезличенных данных должен полностью соответствовать

составу обезличиваемых персональных данных);
- сохранение структурированности обезличиваемых персональных данных;
- сохранение семантической целостности обезличиваемых персональных данных;
- анонимность отдельных данных не ниже заданного уровня (количества возможных сопоставлений обезличенных данных между собой для деобезличивания как, например, k-anonymity – свойство, которым обладают определенные анонимные данные).

2) требованиям к свойствам метода обезличивания:
- обратимость (возможность проведения деобезличивания);
- возможность обеспечения заданного уровня анонимности;
- увеличение стойкости при увеличении объема обезличиваемых персональных данных.

3.11. Удаление, уничтожение ПДн

Удалением, уничтожением ПДн являются действия, в результате которых становится невозможным восстановить содержание ПДн.

Компания обязана прекратить обработку ПДн субъекта данных и произвести уничтожение ПДн, в следующих случаях:
- цели обработки ПДн достигнуты;
- ПДн больше не требуются для достижения целей, в которых они были получены;
- истекли сроки хранения ПДн;
- истек срок согласия на обработку ПДн;
- Компанией выявлены случаи неправомерной обработки ПДн, в том числе по обращению Субъекта данных, когда обеспечить правомерность обработки ПДн невозможно;
- Компанией установлена избыточность состава ПДн по отношению к заявленным целям обработки, когда обеспечить правомерность обработки ПДн невозможно;
- субъект данных отозвал свое согласие на обработку ПДн и у Компании отсутствуют иные законные основания для продолжения обработки ПДн субъекта данных без его согласия.

В случае достижения цели обработки ПДн и отсутствия иных оснований на их обработку Компания обязана прекратить обработку и уничтожить ПДн в срок, не превышающий 30 (тридцати) календарных дней с даты достижения цели обработки ПДн.

В случае выявления неправомерной обработки ПДн Компания в срок, не превышающий 3 (трех) рабочих дней с даты этого выявления, обязана прекратить неправомерную обработку ПДн. В случае если обеспечить правомерность обработки ПДн невозможно, Компания в срок, не превышающий 10 (десяти) рабочих дней с даты выявления неправомерной обработки ПДн, обязана удалить такие ПДн.

В случае отзыва субъектом данных согласия на обработку ПДн, если у Компании отсутствуют иные законные основания для продолжения обработки ПДн субъекта данных без его согласия, Компания обязана прекратить обработку ПДн в срок, не превышающий 30 (тридцати)

календарных дней с даты поступления отзыва.
В случае отсутствия возможности уничтожения ПДн в течение вышеуказанных сроков Компании осуществляет блокирование таких ПДн и уничтожает ПДн в срок не более чем 6 (шесть) месяцев.
В случае уничтожения ПДн по обращению в Компании субъекта данных Компания обязана уведомить их о предпринятых мерах по уничтожению ПДн в сроки, установленные законодательством.
Контроль за соблюдением сроков уничтожения ПДн осуществляется руководителями структурных подразделений Компании.

3.12. Методы уничтожения:

- уничтожение ПДн в электронном виде осуществляется путем удаления записей в ИС;
- уничтожение ПДн в электронном виде может осуществляться путем заполнения данных сгенерированными цифровыми, буквенными и символьными значениями;
- уничтожение материальных носителей ПДн осуществляется путем измельчения, термической обработки, размагничивания, механического разрушения и т.п.

3.13. Требования к технологии уничтожения, удаления ПДн:

- уничтожение ПДн рекомендуется осуществлять путем гарантированного удаления без возможности восстановления записей.

4. ТРЕБОВАНИЯ К СОГЛАСИЮ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1 Общие требования

Согласие на обработку ПДн должно отвечать следующим требованиям:

- должно быть конкретным, информированным и выраженным недвусмысленно;
- может быть дано субъектом данных в любой позволяющей подтвердить факт его получения форме;
- должно быть дано свободно, своей волей и в своем интересе.

Обработка ПДн субъектов данных в целях продвижения товаров, работ, услуг на рынке путем прямых контактов с субъектом данных с помощью средств связи должна осуществляться только при условии предварительного согласия субъекта данных. При этом необходимо обеспечить наличие доказательственной базы получения такого согласия.

4.2 Получение согласия от субъекта данных

Согласие может быть получено в как в бумажном виде, так и в любой форме с использованием сервисов Компании, позволяющей подтвердить факт его получения. Например:

- нажатие субъектом ПД на кнопку «Подтверждаю», «Согласен», «Принимаю», «Продолжить» и т.п. после процедуры ознакомления с текстом документа,

регламентирующего обработку ПДн;

- заполнение чек-бокса рядом с текстом документа, регламентирующего обработку ПДн, в графическом интерфейсе.

4.3 Обеспечение доказательств наличия правовых оснований на обработку ПДн

Компания осуществляет учет и хранение согласий в течение срока действия согласия.
Подтверждением факта получения согласия на бумажном носителе является скан-копия подписанного документа.
Хранение скан-копий подписанных документов осуществляется в структурном подразделении, в интересах деятельности которого осуществляется сбор ПДн.
В целях обеспечения подтверждения получения/отзыва согласий в электронном виде, в ИС Компании рекомендуется реализовать функции учета полученных согласий в журналах аудита ИС и хранения подтверждений (с возможностью их выгрузки для последующей печати), содержащих следующую информацию:

- идентификационные данные субъекта данных;
- признак акцепта согласия / отзыва согласия;
- дату и время акцепта согласия / отзыва согласия.

В части согласий, имеющих длительные сроки действия, превышающие сроки хранения в ИС журналов аудита и атрибутов, из ИС может осуществляться выгрузка и формирование подтверждений в формат электронного документа с последующей записью файла в эту же ИС.

5. ВНЕСЕНИЕ ИЗМЕНЕНИЙ

5.1. Общее руководство и контроль исполнения требований настоящей Политики возложены менеджера ИБ.
5.2. Ответственным за актуализацию Политики является менеджер ИБ. В целях поддержания эффективности СМИБ данный документ должен пересматриваться при необходимости, но не реже одного раза в три года.