

ПОЛИТИКА ЗАЩИТЫ ДАННЫХ

1. ОБЩИЕ ПОЛОЖЕНИЯ.

Политика («Политика») разработана в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» («Закон о персональных данных») и является внутренним основополагающим нормативным документом ООО «Валстед Ист (СЕ)» в Российской Федерации, которая определяет ее основные направления деятельности в части обработки и защиты персональных данных.

Для целей настоящей Политики под Компанией/Валстед/Оператором понимается ООО «Валстед Ист (СЕ)» с местонахождением, 125040, г. Москва, ул. Скаковая, д. 17, корп. 2, Российская Федерация, ИНН 7710652860, КПП 771401001.

Политика направлена на реализацию требований законодательства об обработке и защите персональных данных, а также на защиту прав и свобод граждан при обработке Компанией их персональных данных.

В Политике определены следующие термины:

Безопасность персональных данных - состояние защищенности персональных данных от неправомерных действий, характеризующееся способностью пользователей, технических средств и информационных систем обеспечивать конфиденциальность, целостность и доступность персональных данных при их обработке независимо от их формы.

Конфиденциальность персональных данных – обязательное для соблюдения Оператором или иным получившим доступ к персональным данным лицом требование не разглашать их третьим лицам и не допускать их распространения при отсутствии согласия субъекта персональных данных или иного законного основания.

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых в автоматическом или ручном режиме с персональными данными, включая, но не ограничиваясь сбором, записью, систематизацией, накоплением, хранением, уточнением (обновлением, изменением), извлечением, использованием, распространением (в том числе передача), обезличивание, блокирование и уничтожение персональных данных.

Оператор персональных данных – юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующее и (или) осуществляющее обработку персональных данных, а также определяющее цели и объем обработки персональных данных.

Персональные данные (ПДн) — любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (далее — «Субъект ПДн»).

Специальные категории персональных данных — любая информация, которая касается расовой или этнической принадлежности, национальности, политических взглядов, религиозных или философских убеждений, состояния здоровья или сексуальной ориентации.

Субъекты персональных данных («Субъект ПДн») – работники Компании и иные категории субъектов ПДн, указанные в локальных правовых актах каждой из Компаний, ПДн которых обрабатывается в Компании.

Трансграничная передача персональных данных – любая передача персональных данных иностранному государству, иностранному государственному органу и/или иностранному физическому или юридическому лицу.

2. ПРАВОВЫЕ ОСНОВАНИЯ ДЛЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Компания обрабатывает персональные данные, если выполняется хотя бы одно из следующих условий:

- обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;
- обработка персональных данных необходима для достижения целей, установленных международным договором Российской Федерации, либо необходима для реализации и выполнения функций, полномочий и обязанностей, возлагаемых действующим законодательством Российской Федерации на оператора;
- обработка персональных данных необходима для осуществления правосудия, исполнения судебного акта, акта иного органа или должностного лица, подлежащего исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве;
- Обработка персональных данных необходима для исполнения договора, стороной данных либо выгодоприобретателем или поручителем которого является субъект персональных, а также для заключения договора по инициативе субъекта персональных данных либо договора, в соответствии с которым персональные данные субъект данных будет бенефициаром или поручителем;
- обработка персональных данных необходима для реализации прав и законных интересов оператора или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;
- Обработка общедоступных персональных данных;
- Обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

Примерами упомянутых выше «законных интересов» являются:

- Предлагать информацию о Компании (включая события и вакансии) и/или услуги, в том числе лицам, которые посещают веб-сайт Компании.

- Для предотвращения мошенничества или преступной деятельности и для защиты ИТ-систем.
- Проведение и анализ маркетинговых мероприятий.
- Выполнение обязательств по корпоративной и социальной ответственности.
- Соответствие нормативным актам или нормативным указаниям.
- Для передачи персональных данных другим подразделениям Walstead Group.

Обработка Компанией особых категорий персональных данных, касающихся расы, национальности, политических взглядов, религиозных или философских убеждений.

ЭФС, состояние здоровья, сексуальная ориентация допускаются в случаях, когда: субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных;

Персональные данные сделаны общедоступными субъектом персональных данных;

Обработка персональных данных осуществляется в соответствии с действующим законодательством о государственной социальной помощи, трудовым законодательством, действующим законодательством Российской Федерации о пенсиях для государственного пенсионного обеспечения, о трудовых пенсиях;

Обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия субъекта персональных данных невозможно

Обработка персональных данных осуществляется в лечебно-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг, при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным соблюдать врачебную тайну в соответствии с действующим законодательством Российской Федерации;

Обработка персональных данных необходима для установления или реализации прав субъекта персональных данных или третьих лиц, а также в связи с осуществлением правосудия.

Обработка персональных данных осуществляется в соответствии с действующим законодательством об обязательных видах страхования, действующим законодательством о страховании. Обработка специальных категорий персональных данных подлежит немедленному прекращению, если устранены причины их обработки, если иное не установлено федеральным законом.

3. ПРАВА СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

Субъекты ПДн имеют следующие права:

- право на получение информации об обработке своих Персональных данных в Компании;

- право назначать своих представителей для защиты своих прав;
- право требовать от Оператора исправления, блокирования или уничтожения Персональных данных в случае, если Персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не нужны для заявленной цели обработки, и имеет право принимать предусмотренные законом меры для защиты своих прав;
- право требовать уведомления Компанией всех третьих лиц, которым были переданы неверные или неполные ПДн, обо всех изменениях ПДн;
- право на безвозмездный доступ к своим ПДн, в том числе право на получение копии любой записи ПДн, если иное не предусмотрено федеральными законами;
- право на отзыв согласия на обработку ПДн;
- право возражать против решений, принимаемых исключительно на основании автоматизированной обработки их ПДн, а также получать от Оператора разъяснения относительно способов защиты субъектом ПДн своих прав и законных интересов; право на обжалование действий или бездействия Оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке;
- право на жалобу в соответствующий орган по защите данных (Роскомнадзор).

4. ОСНОВНЫЕ ПРИНЦИПЫ

Ключевые принципы, которые применяются к обработке персональных данных:

а) Прозрачность

Все субъекты данных могут решить, предоставлять ли свои персональные данные для обработки. Субъект данных имеет право знать цели и способы обработки персональных данных, наименование и местонахождение оператора данных, получателей персональных данных, лиц, имеющих доступ к персональным данным, срок действия обработки и хранение персональных данных, а также любая другая информация, необходимая для обеспечения прозрачной обработки персональных данных.

б) Законное правовое основание

Персональные данные обрабатываются на законной и справедливой основе. В частности, обработка персональных данных должна осуществляться с согласия субъекта данных (если не применяются определенные правовые исключения), которое предоставляется добровольно, по доброй воле субъекта данных и в собственных интересах субъекта данных, оператора данных или другой стороны. получивший доступ к персональным данным, не вправе разглашать или распространять такие данные третьим лицам без согласия субъекта данных, если иное не допускается законодательством.

в) Целевое ограничение

Обработка персональных данных должна ограничиваться достижением целей, которые должны быть конкретными, заранее определенными и законными. Обработка, не соответствующая целям такой обработки, запрещена.

г) Минимизация данных

Объем и содержание обрабатываемых персональных данных должны полностью соответствовать предполагаемым целям такой обработки данных. Персональные данные не должны быть избыточными или нерелевантными заявленным целям обработки данных.

д) Соразмерность

Обработка персональных данных должна обеспечивать, чтобы такие персональные данные были точными, достаточными, адекватными и актуальными, обновлялись в соответствии с целями обработки данных.

е) Удержание

Персональные данные, которые были обработаны, должны быть уничтожены или анонимизированы после того как цель обработки данных достигнута либо утратила силу, актуальность или необходимость, если иное не установлено федеральными законами.

5. КАТЕГОРИИ СУБЪЕКТОВ ДАННЫХ

В ходе своей основной деятельности Компания обрабатывает Персональные данные следующих субъектов (включая, но не ограничиваясь):

- Кандидаты на вакантные должности;
- Работники, в том числе физические лица, с которыми расторгнуты трудовые договоры,
- члены семей сотрудников;
- Поставщики услуг, клиенты, потенциальные клиенты, сотрудники и иные субъекты ПДн клиентов Компании, ПДн которых обрабатываются в рамках договора на оказание услуг,
- Посетители сайтов, работающих в пользу Компании.

6. ОСНОВНЫЕ МЕРЫ БЕЗОПАСНОСТИ

К основным мерам безопасности персональных данных в целях защиты персональных данных при их обработке относятся:

- принятие документов, определяющих политику Оператора в отношении обработки персональных данных, издание внутренних регламентов в области обработки персональных данных и иных внутренних нормативных документов, устанавливающих порядок предотвращения и выявления нарушений законодательства Российской Федерации и ликвидации последствий таких нарушений.
- осуществление внутреннего контроля для оценки соблюдения Закона о ПДн, а также принятых в соответствии с ним положений и требований о защите персональных данных, политики Оператора в отношении обработки персональных данных и его внутренних документов.
- оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения требований законодательства, размер такого выявленного вреда и меры безопасности, принимаемые Оператором.
- ознакомление работников Компании, непосредственно осуществляющих обработку персональных данных, с требованиями Закона о ПДн.
- организация и контроль деятельности, связанной с приемом и обработкой заявлений и запросов субъектов персональных данных или их представителей (в соответствии с локальными правовыми нормами, принятыми в Компании);
- иные меры безопасности персональных данных, применяемые Компанией (описаны в Приложении №1 к настоящей Политике).

7. ОТВЕТ НА ЗАПРОС СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

Субъекты данных имеют право направлять Компании следующие запросы или требования:

а) Запрос на получение информации об обработке ПДн, в том числе:

- подтверждение обработки ПДн Компанией;
- правовые основания и цели обработки ПДн;
- методы, используемые Компанией для обработки ПДн;
- наименование и место нахождения Общества и сведения о лицах (кроме работников Общества), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с Обществом или на основании федерального закон;
- обрабатываемые ПДн, относящиеся к рассматриваемому Субъекту ПДн, и источник, из которого они получены, если иной порядок представления таких сведений не установлен федеральным законом;

- срок обработки ПДн, в том числе срок хранения данных;
 - порядок осуществления субъектом ПДн прав, предусмотренных Законом о ПДн;
 - информация о любой фактической или планируемой трансграничной передаче ПДн;
 - имя, фамилия или адрес лица, осуществляющего обработку ПДн по поручению Компании, если обработка была или предполагается возложить на такое лицо.
- б) требовать уточнения, блокирования или уничтожения его персональных данных, если персональные данные являются неполными, устаревшими, неверными, незаконно полученными или не являются необходимыми для заявленной цели обработки либо если цель обработки достигнута;
- в) возражать против решения, принятого исключительно на основании автоматизированной обработки ПДн;
- г) Отозвать согласие на обработку ПДн.

Запросы субъектов ПДн (или их представителей) могут быть направлены в Компанию в письменной форме через Почту России или в электронной форме в соответствии с действующим законодательством Российской Федерации, лично субъектом ПДн, при посещении Компании и по телефону.

8. ПЕРЕДАЧА ПЕРСОНАЛЬНЫХ ДАННЫХ

Валстед может делиться личными данными с другими компаниями в рамках Walstead Group в рамках международных обязательств.

Оператор не передает личную информацию третьим лицам, за исключением случаев, когда это необходимо для наших законных профессиональных и деловых нужд, для выполнения запросов клиентов, для выполнения договорных обязательств, как это требуется или разрешено законом или профессиональными стандартами (например, размещение и поддержка ИТ-приложений, предоставление определенных форм страхования для фирм-членов и их клиентов, оказание помощи в услугах по привлечению клиентов и в других случаях, необходимых для продолжения ведения бизнеса Оператора).

Вложения:

Приложение № 1 Меры безопасности

Приложение № 1 - Меры безопасности

1. Контроль доступа (ИТ-системы, приложения)

Целью контроля доступа к ИТ-системам и приложениям является предотвращение использования неавторизованными лицами систем обработки данных, предназначенных для обработки данных.

Принимаемые меры:

- Доступ к ИТ-системам и приложениям контролируется с помощью стандартной аутентификации, такой как пароль для учетной записи и разрешения, адаптированные к роли конкретного лица. Это в равной степени относится к администраторам, разработчикам и пользователям.
- Для систем, которые могут поддерживать сложность пароля, все пароли должны состоять не менее чем из 8 символов, содержать 3 из 4 конфигураций сложности (верхний регистр, цифра, специальный символ и нижний регистр) и должны меняться не реже одного раза в 60 дней.
- Там, где это возможно, внедряются средства контроля, гарантирующие, что пароли не будут использоваться повторно в течение как минимум одного года или после восьми смен паролей.
- Политика паролей применяется ко всем учетным записям пользователей сети Walstead.
- Ограниченное количество неправильных попыток входа в систему.
- Блокировка экрана с защитой паролем.
- Внутренняя сеть защищена от внешних атак брандмауэром уровня 7.

- Сегментация внутренней сети в целях безопасности, т. е. ограничение доступа в Интернет, сегменты беспроводной сети.
- Жесткие диски мобильных компьютеров зашифрованы.
- Протоколы аутентификации и шифрования для разрешения доступа к беспроводным сетям.
- Мобильные устройства требуют защиты паролем или PIN-кодом.
- Удаленный доступ сотрудников и постоянных подрядчиков к внутренней сети Walstead осуществляется по зашифрованному каналу и требует использования принадлежащего Walstead оборудования с утвержденной конфигурацией оборудования, которая автоматически проверяется перед установлением соединения.
- Доступ третьих лиц разрешен только к выделенным изолированным сегментам сети.

2. Контроль доступа к персональным данным

Целью контроля доступа к персональным данным является обеспечение того, чтобы только лица, уполномоченные на обработку персональных данных, могли получить доступ к персональным данным, чтобы объем и средства обработки данных соответствовали выданному письменному разрешению и требованиям закона о защите данных, и что персональные данные не могли быть прочитаны, скопированы, изменены или удалены без соответствующего разрешения.

Принимаемые меры:

- Для аутентификации доступа необходимо использовать индивидуальный идентификатор пользователя и пароль.
- Концепция владельца информации – возложенная на отдельных лиц ответственность за соответствующие наборы данных.
- Процедура управления доступом, включая предоставление разрешений и проверку доступа.
- Процедура лишения доступа в случае увольнения сотрудника или смены должности.
- Разделение сред тестирования приложений и производственных сред, псевдонимизация тестовых данных
- Политика очистки рабочего стола/чистого экрана.
- Защита паролем файлов, содержащих неструктурированные личные данные.

3. Контроль доступности данных

Целью контроля доступности данных является обеспечение защиты персональных данных от случайного уничтожения или потери.

Принимаемые меры:

- Обработка данных происходит строго в защищенной документированной среде.
- Процедура резервного копирования данных (с указанием периодичности, носителя, периода хранения и места).
- Центральная система резервного копирования с дисковыми массивами и библиотекой на дата - картриджах.
- Дисковые массивы с конфигурацией RAID.
- Регулярная репликация данных за пределы площадки.
- Защита от перегрузки.
- Источники бесперебойного питания (ИБП).
- Электрогенераторы в месте нахождения центрального сервера.
- Модули AntiVirus, AntiSpyware, AntiMalware на пограничном брандмауэре.
- Антивирусная защита с обязательными регулярными обновлениями на серверах и рабочих станциях.
- Обновления и исправления, устанавливаемые на регулярной основе с использованием механизма управляемого централизованно.
- Мониторинг производительности и доступности систем с включенным автоматическим оповещением.
- Техническое обслуживание и профилактические мероприятия.
- Поддержание избыточной вычислительной мощности для использования в экстренных случаях.
- Резервное оборудование/услуги для устранения единых точек отказа.
- Внедрение планов обеспечения непрерывности бизнеса и аварийного восстановления.

4. Работа с персоналом

Целью кадрового контроля является обеспечение наличия процессов, обеспечивающих надежность работы всех сотрудников, имеющих доступ к персональным данным.

Принимаемые меры:

- Разумные меры для обеспечения надежности работы всех сотрудников, которые будут иметь доступ к персональным данным, в том числе:
 - Проведение проверок биографических данных
 - Заключение соглашений о конфиденциальности и соблюдение политик и стандартов (нарушение которых может привести к дисциплинарным взысканиям, включая увольнение)
 - Для обработки персональных данных требуется индивидуальное разрешение.
- Обучение защите данных и безопасности данных при вступлении в должность и, по крайней мере, ежегодно впоследствии .
 - Определение правил допустимого использования компьютерной техники и информационных систем.

5. Удаление персональных данных

Целью контроля за утилизацией является обеспечение безопасного удаления персональных данных.

Принимаемые меры:

- Политика хранения данных.
- Уничтожение данных в соответствии с требованиями Оператора.
- Надежная утилизация бумажных отходов.
- Безопасное стирание, размагничивание или физическое уничтожение или выдача команд ОС для удаления данных, хранящихся на оборудовании и электронных носителях.
- Безопасный вывод из эксплуатации ИТ-оборудования.
- Порядок удаления персональных данных по требованию объекта данных/по указанию Оператора.