

Политика
Общества с ограниченной ответственностью «Велнес Бьюти Студио»
по информационной безопасности

Юридический адрес: 119296, г. Москва, Ленинский проспект, дом 67, корпус 2
Фактический адрес: 119296, г. Москва, Ленинский проспект, дом 67, корпус 2

Политика по информационной безопасности (далее по тексту Политика) Общества с ограниченной ответственностью «Велнес Бьюти Студио» (далее по тексту Общество) разработана в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных.

Политика разработана в соответствии с требованиями Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и постановления Правительства Российской Федерации от 11 ноября 2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», на основании «Рекомендаций по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденных Заместителем директора ФСТЭК России от 15.02.2008 г.

В Политике определены требования к персоналу по безопасности информационных систем персональных данных (далее ИСПД), степень ответственности персонала, структура и необходимый уровень защищенности, статус и должностные обязанности сотрудников, ответственных за обеспечение безопасности персональных данных в ИСПД Общества.

Политика Общества в отношении обработки персональных данных определяет позицию и намерения Общества в области обработки и защиты персональных данных с целью соблюдения и защиты прав и свобод каждого человека и, в особенности, права на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени.

Действие Политики распространяется на все персональные данные субъектов, обрабатываемые в Обществе с применением средств автоматизации и без применения таких средств. К настоящей Политике имеет доступ любой субъект персональных данных.

1. Определения

Персональные данные - любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (гражданину). К такой информации, в частности, можно отнести: ФИО, год, месяц, дата и место рождения, адрес, сведения о семейном, социальном, имущественном положении, сведения об образовании, профессии, доходах, сведения о состоянии здоровья, а также другую информацию.

Обработка персональных данных - любое действие (операция) или совокупность действий (операций) с персональными данными, совершаемых с использованием средств автоматизации или без использования таких средств. К таким действиям (операциям) можно отнести: сбор, получение, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Субъекты персональных данных: Общество обрабатывает персональные данные следующих лиц: работников Общества; субъектов, с которыми заключены договоры гражданско-правового характера; кандидатов на замещение вакантных должностей Общества; клиентов Общества; зарегистрированных пользователей сайта Общества www.beautypractice.ru; представителей юридических лиц; поставщиков (индивидуальных предпринимателей).

2. Общие положения

Целью настоящей Политики является обеспечение безопасности объектов защиты Общества от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности сохранности персональных данных.

Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

Информация и связанные с ней ресурсы должны быть доступны для авторизованных пользователей. Должно осуществляться своевременное обнаружение и реагирование на угрозу безопасности персональных данных.

Должно осуществляться предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения данных.

Состав объектов защиты представлен в Перечне персональных данных, подлежащих защите.

Политика информационной безопасности утверждена руководителем ООО «Велнес Бьюти Студио» и введена в действие приказом генерального директора.

Общество обрабатывает персональные данные только при наличии хотя бы одного из следующих условий:

обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных; обработка персональных данных необходима для достижения целей, предусмотренных законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей; обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем; обработка персональных данных необходима для осуществления прав и законных интересов Общества или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных; осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе; осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

Общество вправе поручить обработку персональных данных граждан третьим лицам на основании заключаемого с этими лицами договора. Лица, осуществляющие обработку

персональных данных по поручению Общества, обязуются соблюдать принципы и правила обработки и защиты персональных данных, предусмотренные Федеральным законом № 152-ФЗ «О персональных данных». Для каждого лица определены перечень действий (операций) с персональными данными, которые будут совершаться юридическим лицом, осуществляющим обработку персональных данных, цели обработки, установлена обязанность такого лица соблюдать конфиденциальность и обеспечивать безопасность персональных данных при их обработке, а также указаны требования к защите обрабатываемых персональных данных.

В случаях, установленных законодательством Российской Федерации, Общество вправе осуществлять передачу персональных данных граждан.

В целях информационного обеспечения в Обществе могут создаваться общедоступные источники персональных данных работников, в том числе справочники и адресные книги. В общедоступные источники персональных данных с согласия работника могут включаться его фамилия, имя, отчество, дата и место рождения, должность, номера контактных телефонов, адрес электронной почты, данные об образовании, опыте работы, личная фотография для публикации на сайте анкетная и в процессе оказания услуг по профилю Общества. Сведения о работнике должны быть в любое время исключены из общедоступных источников персональных данных по требованию работника либо по решению суда или иных уполномоченных государственных органов.

3. Область действия

Требования настоящей Политики распространяются на всех сотрудников Общества (штатных, временных, работающих по контракту и т.п.), а также всех прочих лиц (подрядчики, аудиторы и т.п.).

4. Права субъекта персональных данных

Гражданин, персональные данные которого обрабатываются Обществом, имеет право получать от Общества подтверждение факта обработки персональных данных Обществом; правовые основания и цели обработки персональных данных; сведения о применяемых Обществом способах обработки персональных данных; наименование и местонахождения Общества; сведения о лицах, которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Обществом или на основании федерального закона; перечень обрабатываемых персональных данных, относящихся к гражданину, от которого поступил запрос и источник их получения, если иной порядок предоставления таких данных не предусмотрен федеральным законом; сведения о сроках обработки персональных данных, в том числе о сроках их хранения; сведения о порядке осуществления гражданином прав, предусмотренных Федеральным законом «О персональных данных» № 152-ФЗ; информацию об осуществляемой или о предполагаемой трансграничной передаче персональных данных; наименование и адрес лица, осуществляющего обработку персональных данных по поручению Общества; иные сведения, предусмотренные Федеральным законом «О персональных данных» № 152-ФЗ или другими федеральными законами; требовать уточнения своих 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; отозвать свое согласие на обработку персональных данных; требовать устранения неправомерных действий Общества в отношении его персональных данных; обжаловать действия или бездействие Общества в Федеральную службу по надзору в сфере связи, информационных технологий и

массовых коммуникаций (Роскомнадзор) или в судебном порядке в случае, если гражданин считает, что Общество осуществляет обработку его персональных данных с нарушением требований Федерального закона № 152-ФЗ «О персональных данных» или иным образом нарушает его права и свободы; на защиту своих прав и законных интересов.

5. Система защиты персональных данных

Система защиты персональных данных Общества и необходимый уровень защищенности персональных данных строится на основании:

- Отчета о результатах проведения внутренней проверки;
- Перечня персональных данных, подлежащих защите;
- Положения о разграничении прав доступа к обрабатываемым персональным данным.

В Обществе составлен список используемых технических средств защиты, а также программного обеспечения участвующего в обработке персональных данных.

Система защиты персональных данных включает в себя:

- антивирусные средства для рабочих станций пользователей и серверов.

Список функций защиты включает в себя:

- управление и разграничение доступа пользователей;
- регистрацию и учет действий с информацией;
- обеспечение целостности данных;
- возможность производить обнаружений вторжений.

Список используемых средств поддерживается в актуальном состоянии. При изменении состава технических средств защиты, соответствующие изменения вносятся в Список и утверждаются руководителем Общества.

Система антивирусной защиты предназначена для обеспечения антивирусной защиты серверов и АРМ пользователей Общества.

Средства антивирусной защиты предназначены для реализации следующих функций:

- антивирусный мониторинг;
- антивирусное сканирование;
- централизованную / удаленную установку / деинсталляцию антивирусного продукта, настройку, администрирование, просмотр отчетов и статистической информации по работе продукта;
- автоматизированное обновление антивирусных баз;
- ограничение прав пользователя на остановку исполняемых задач и изменения настроек антивирусного программного обеспечения;
- автоматический запуск сразу после загрузки операционной системы.

Подсистема реализуется путем внедрения специального антивирусного программного обеспечения на все элементы ИСПД.

6. Пользователи ИСПД.

В ИСПД назначены сотрудники, участвующие в обработке и хранении ПД, как операторы АРМ.

Данные о группах пользователей, уровне их доступа и информированности отражены в Положении о разграничении прав доступа к обрабатываемым персональным данным.

Оператор АРМ, сотрудники Общества, осуществляющие обработку ПД. Обработка ПД включает: возможность просмотра ПД, ручной ввод ПД в систему ИСПД, формирование справок и отчетов по информации, полученной из ИСПД. Оператор не имеет полномочий для управления подсистемами обработки данных и СЗПД.

Оператор ИСПД обладает следующим уровнем доступа и знаний:

- обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству ПД;
- располагает конфиденциальными данными, к которым имеет доступ.

Операторами ИСПД в силу должностных обязанностей в Обществе являются: Генеральный директор Общества, Управляющий директор Общества, Главный врач Общества, Главный бухгалтер Общества, администраторы, старший администратор, специалисты (врачи и медсестры).

Все сотрудники Общества, являющиеся пользователями ИСПД, знают и строго выполняют установленные правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности персональных данных.

Сотрудникам запрещается устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и носители информации, а также записывать на них защищаемую информацию.

Сотрудникам запрещается разглашать защищаемую информацию, которая стала им известна при работе с информационными системами Общества, третьим лицам.

При работе с персональными данными сотрудники Общества обязаны обеспечить отсутствие возможности просмотра данных третьими лицами с мониторов или терминалов.

При завершении работы с ИСПД сотрудники обязаны защитить мониторы или терминалы с помощью блокировки ключом или эквивалентного средства контроля, например, доступом по паролю, если не используются более сильные средства защиты.

Сотрудники Общества проинформированы об угрозах нарушения режима безопасности ПД и ответственности за его нарушение, ознакомлены с утвержденной процедурой наложения дисциплинарных взысканий на сотрудников, которые нарушили принятые политику и процедуры безопасности персональных данных.

Сотрудники обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы ИСПД, могущих повлечь за собой угрозы безопасности персональных данных, а также о выявленных ими событиях, затрагивающих

безопасность персональных данных, руководству подразделения и лицу, отвечающему за немедленное реагирование на угрозы безопасности персональных данных.

Получить разъяснения по интересующим Вас вопросам обработки Ваших персональных данных, можно обратившись лично в Общество либо направив официальный запрос по Почте России по адресу: 119296, г. Москва, Ленинский проспект, дом 67, корпус 2. В случае направления официального запроса в Общество в тексте запроса необходимо указать: ФИО; номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе; сведения, подтверждающие Ваше участие в отношениях с Обществом либо сведения, иным способом подтверждающие факт обработки персональных данных Обществом; подпись гражданина (или его законного представителя). Если запрос отправляется в электронном виде, то он должен быть оформлен в виде электронного документа и подписан электронной подписью в соответствии с законодательством РФ.

На сайте www.beautypractice.ru публикуется актуальная версия «Политики Общества с ограниченной ответственностью "Велнес Бьюти Студио» по информационной безопасности».