Положение об обработке и обеспечении безопасности персональных данных в физкультурно-оздоровительных клубах сети «FreshFit&Spa»

Настоящее Положение разработано в соответствии с законодательством Российской Федерации о персональных данных (далее – ПДн) и нормативно-методическими документами уполномоченных органов государственной власти по вопросам безопасности ПДн, в том числе при их обработке в информационных системах персональных данных (далее – ИСПДн) индивидуальным предпринимателем Индивидуальным предпринимателем Романовским Всеволодом Вячеславовичем, (физкультурно-оздоровительный клуб Freshfit&Spa (Фреш Фитнес), действующей на основании ОГРНИП № 320265100077880 (далее – Оператор).

Основными нормативно-правовыми и методическими документами, на которых базируется настоящее Положение, являются:

- Федеральный закон Российской Федерации от 27.07.2006 г. № 152-ФЗ «О персональных данных» (далее – ФЗ «О персональных данных»).
- Постановление Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Постановление Правительства Российской Федерации от 15.09.2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

Для осуществления мероприятий по обеспечению и контролю безопасности персональных данных, обработки обращений субъектов ПДн и взаимодействия с уполномоченным органом по защите прав субъектов ПДн приказом руководителя Оператора назначается работник, ответственный за организацию обработки персональных данных и работник, ответственный за обеспечение безопасности ПДн при их обработке в ИСПДн Оператора.

Назначение и Область действия

Настоящее Положение предназначено для организации Оператором процессов обработки и обеспечения безопасности ПДн согласно требованиям действующего законодательства РФ.

Действие настоящего Положения распространяется на все процессы по сбору, систематизации, накоплению, хранению, уточнению, использованию, распространению (в том числе передаче), обезличиванию, блокированию, уничтожению ПДн, осуществляемые с использованием средств автоматизации и без их использования.

Положение обязательно для ознакомления и исполнения всеми работниками Оператора.

Принципы и условия обработки ПДн

Принципы обработки ПДн

Обработка ПДн осуществляется на основе следующих принципов:

- обработка ПДн осуществляется на законной и справедливой основе;
- обработка ПДн ограничивается достижением конкретных, заранее определенных и законных целей;
- содержание и объем обрабатываемых ПДн соответствуют заявленным целям обработки, обрабатываемые ПДн не являются избыточными по отношению к заявленным целям обработки;
- при обработке ПДн обеспечивается точность ПДн и их достаточность, а также актуальность ПДн по отношению к заявленным целям их обработки;
- обрабатываемые ПДн подлежат уничтожению или обезличиванию по достижению целей обработки или в случае утраты необходимости в достижении этих целей;

- обработка ПДн осуществляется с согласия субъекта ПДн или его законного представителя.

Условия обработки ПДн

Обработка персональных данных может осуществляться Оператором только с согласия субъектов персональных данных, за исключением случаев, предусмотренных законодательством Российской Федерации, в частности:

- обработка персональных данных осуществляется на основании федерального закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия оператора;
- обработка персональных данных осуществляется в целях исполнения договора, одной из сторон которого является субъект персональных данных;
- обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;
- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно.

В следующих случаях требуется письменное согласие субъекта на обработку его ПДн:

- включение ПДн субъекта в общедоступные источники ПДн;
- обработка специальных категорий ПДн, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни;
- обработка биометрических ПДн (сведений, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность);
- трансграничная передача ПДн на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов ПДн[1];
- принятие на основании исключительно автоматизированной обработки ПДн решений, порождающих юридические последствия в отношении субъекта ПДн или иным образом затрагивающих его права и законные интересы.

В случае недееспособности субъекта ПДн согласие на обработку его ПДн дает в письменной форме законный представитель субъекта ПДн.

Формы письменного согласия субъекта на обработку его ПДн для различных категорий субъектов, персональные данные которых обрабатываются Оператором, и различных целей обработки таких данных, приведены в приложении А.

В случае если Оператор на основании договора поручает обработку персональных данных другому физическому или юридическому лицу, существенным условием договора является обязанность обеспечения указанным лицом конфиденциальности персональных данных и безопасности персональных данных при их обработке, а также обязательное указание целей передачи персональных данных и перечня видов, передаваемых на обработку персональных данных.

Операторами и третьими лицами, получающими доступ к ПДн, должна обеспечиваться конфиденциальность таких данных.

Требования к обработке ПДн

Обязанности Оператора

В соответствии с требованиями Федерального закона «О персональных данных» Оператор обязан:

- предоставлять субъекту ПДн или его законному представителю по запросу информацию, касающуюся обработки его ПДн, либо на законных основаниях предоставить отказ в течение тридцати дней с даты получения запроса субъекта ПДн или его представителя;

- по требованию субъекта ПДн или его законного представителя уточнять, блокировать или удалять обрабатываемые ПДн, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки в срок, не превышающий семи рабочих дней со дня предоставления субъектом ПДн или его представителем сведений, подтверждающих эти факты;

- в случае достижения цели обработки ПДн незамедлительно прекратить обработку ПДн и уничтожить соответствующие ПДн в срок, не превышающий тридцати дней с даты достижения цели обработки ПДн, если иное не предусмотрено договором, стороной которого является субъект ПДн;

- в случае отзыва субъектом ПДн или его законным представителем согласия на обработку ПДн прекратить обработку ПДн и уничтожить ПДн в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено соглашением между Оператором и субъектом ПДн, и уведомить субъекта ПДн или его законного представителя об уничтожении ПДн;

- в случае поступления требования субъекта ПДн или его законного представителя о прекращении обработки ПДн, полученных в целях продвижения товаров, работ, услуг на рынке, немедленно прекратить обработку ПДн.

Процессы обработки ПДн

Обработка ПДн в ИСПДн Оператора включает в себя следующие основные процессы:

- сбор ПДн;
- использование ПДн;
- хранение ПДн в ИСПДн;
- передача ПДн;
- уточнение ПДн;
- блокирование ПДн;
- уничтожение ПДн.

Оператор обязан предоставлять субъекту ПДн или его законному представителю по запросу информацию, касающуюся обработки его ПДн, либо на законных основаниях предоставить отказ в течение тридцати дней с даты получения запроса субъекта ПДн или его представителя. Формы бланков предоставления сведений или отказа в представлении сведений приведены в приложении Б.

- Сбор ПДн

ПДн получаются лично у граждан за исключением случаев получения ПДн из общедоступных источников (в том числе справочников, адресных книг).

Уведомление субъекта об обработке ПДн, полученных из общедоступных источников, не осуществляется.

Оператор может получать, обрабатывать и приобщать к личному делу работника данные о состоянии его здоровья при отсутствии письменного согласия, если обработка ПДн осуществляется или необходима:

- для защиты жизни, здоровья или иных жизненно важных интересов работника Оператора, либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия субъекта ПДн невозможно;

- для установления или осуществления прав работника или третьих лиц, а равно и в связи с осуществлением правосудия;

- в соответствии с законодательством об обязательных видах страхования со страховым законодательством.

○ Использование ПДн

Использование ПДн в ИСПДн Оператора осуществляется работниками Оператора, указанными в Перечне должностей работников, допущенных к работе с ПДн, утверждаемым приказом руководителя Оператора. В данный перечень включаются работники, которым для осуществления своих должностных и функциональных обязанностей необходим доступ к ПДн. В перечне указываются категории ПДн (категории субъектов ПДн), доступ к которым предоставляется работникам, занимающим данную должность.

- Хранение ПДн

Хранение ПДн осуществляется Оператором в соответствии со следующими требованиями:

- хранение ПДн осуществляется таким образом, чтобы в отношении каждой категории ПДн можно было определить места их хранения;
- хранение ПДн осуществляется в форме, позволяющей определить субъекта ПДн не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн;
- не осуществляется несанкционированное копирование ПДн на отчуждаемые носители информации;
- при хранении ПДн в ИСПДн соблюдаются условия, обеспечивающие конфиденциальность и сохранность ПДн;
- исключен несанкционированный доступ к ПДн.

Работники Оператора, обладающие правом доступа к ПДн, несут ответственность за хранение ПДн на своих автоматизированных рабочих местах.

Копирование ПДн на внешние электронные носители, такие как флеш-накопители, внешние жесткие диски, CD, DVD и т. д., осуществляется только для выполнения трудовых обязанностей.

- Передача ПДн

Передача ПДн другим работникам Оператора или третьим лицам осуществляется в следующих случаях:

- если передача ПДн необходима для исполнения работником трудовых обязанностей, связанных с обработкой ПДн;
- если она нужна для исполнения федерального законодательства.

Работники Оператора, допущенные к работе с ПДн, не сообщают устно или письменно ПДн другим работникам или сторонним лицам, которые не участвуют в процессах обработки ПДн.

Ответы на письменные запросы других организаций и учреждений в пределах их компетенции и предоставленных полномочий даются в письменной форме и в том объеме, который позволяет не разглашать излишний объем ПДн.

При передаче ПДн работники Оператора не сообщают ПДн субъекта третьей стороне без письменного согласия субъекта, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта ПДн, а также случаях, предусмотренных Трудовым кодексом Российской Федерации и иными федеральными законами.

Передача ПДн возможна только в том случае, если исключен несанкционированный доступ к ПДн в процессе передачи и обеспечивается конфиденциальность передаваемой информации. Если Оператор на основании договора поручает обработку ПДн другому лицу, существенным условием договора является обязанность обеспечения указанным лицом конфиденциальности и безопасности ПДн при их передаче.

Согласие субъекта на передачу его ПДн не требуется, если сообщение информации или предоставление документов, содержащих ПДн, предусмотрено законодательством Российской Федерации.

Работники Оператора осуществляют передачу ПДн субъекта законному представителю субъекта ПДн, проверив его полномочия в порядке, установленном законодательством Российской Федерации и ограничиваться только теми ПДн, которые необходимы для выполнения указанными представителями их функций.

- Уточнение ПДн

В случае выявления работником Оператора недостоверных ПДн или неправомерных действий с ними работник информирует о данном факте ответственного за организацию обработки ПДн. Ответственный за организацию обработки ПДн в срок, не превышающий трех рабочих дней с даты этого выявления, инициирует выполнение действий по уточнению ПДн.

В случае уточнения (изменения) ПДн необходимо известить третьих лиц, которым ранее были сообщены или переданы неверные или неполные ПДн, обо всех исключениях, исправлениях и дополнениях в них.

Об устранении допущенных нарушений или об уничтожении ПДн требуется уведомить субъекта ПДн или его законного представителя либо уполномоченный орган по защите прав субъектов ПДн в случае, если соответствующую проверку инициировал указанный орган.

- Блокирование ПДн

В случае выявления работником Оператора неправомерной обработки ПДн или выявления неточных ПДн при обращении субъекта или его представителя либо по запросу уполномоченного органа по защите прав субъектов ПДн, Ответственный за организацию обработки ПДн инициирует блокирование ПДн, относящихся к этому субъекту ПДн.

В случаях, если отсутствует возможность уничтожения ПДн, Оператор осуществляет блокирование таких ПДн и обеспечивает уничтожение в срок не более чем шесть месяцев.

- Уничтожение ПДн

ПДн подлежат уничтожению (или обезличиванию) в следующих случаях в указанные сроки:

- по достижении целей обработки ПДн – в 30-дневный срок;
- в случае утраты необходимости в достижении целей обработки ПДн – в 30-дневный срок;
- в случае отзыва субъектом ПДн согласия на обработку своих ПДн – в 30-дневный срок, если иной срок не предусмотрен договором или соглашением между Оператором и субъектом ПДн, либо если Оператор не вправе осуществлять обработку ПДн без согласия субъекта ПДн на основаниях, предусмотренных ФЗ «О персональных данных» или другими федеральными законами.

ПДн подлежат уничтожению (или обезличиванию) в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки ПДн в следующих случаях:

- в случае если ПДн являются неполными, устаревшими, неточными (при условии, что уточнение ПДн невозможно);
- в случае если ПДн являются незаконно полученными;
- в случае если ПДн не являются необходимыми для заявленной цели обработки.

Формы бланков уведомлений об уничтожении или отказе в уничтожении ПДн приведены в приложении Б.

Процесс уничтожения ПДн инициирует Ответственный за организацию обработки ПДн.

Ответственный за организацию обработки ПДн назначает лицо, ответственное за уничтожение ПДн. В случае с бумажными носителями ПДн в качестве лица, ответственного за уничтожение ПДн, назначается владелец

бизнес-процесса. В случае с другими носителями ПДн или если обработка ПДн осуществляется в ИСПДн, то в качестве лица, ответственного за уничтожение ПДн, назначается владелец ИСПДн.

Лицо, ответственное за уничтожение ПДн, производит уничтожение ПДн, оформляет и подписывает Акт об уничтожении ПДн, форма которого представлена в Приложении В. После этого он направляет Акт об уничтожении ПДн Ответственному за организацию обработки ПДн.

Ответственный за организацию обработки ПДн утверждает Акт об уничтожении ПДн и уведомляет субъекта ПДн или его представителя.

В случае уничтожения ПДн по результатам проверки или запроса уполномоченного органа по защите прав субъектов ПДн Ответственный за организацию обработки ПДн уведомляет об уничтожении ПДн субъекта ПДн или его представителя, а также указанный орган.

При уничтожении обеспечивается гарантированное уничтожение ПДн, исключающее возможность их восстановления программными или физическими методами.

Уничтожение бумажных носителей ПДн производится путем измельчения, сжигания или преобразования в целлюлозную массу таким образом, чтобы гарантировать, что их невозможно восстановить.

Обеспечение конфиденциальности ПДн

Оператор и иные лица, обладающие по поручению Оператора правом доступа к ПДн (либо в рамках выполнения должностных обязанностей, либо в рамках договора), принимают на себя и исполняют обязательство не раскрывать третьим лицам и не распространять ПДн без согласия субъекта ПДн, если иное не предусмотрено ФЗ «О персональных данных».

Для обеспечения безопасности персональных данных от совершения неправомочных действий выполняются следующие организационные меры:

- повышение осведомленности работников Оператора по вопросам обеспечения безопасности ПДн при их обработке;
- своевременное выявление нарушений работниками Оператора и уполномоченными лицами требований режима конфиденциальности;
- все работники Оператора, имеющие действующие трудовые отношения, деятельность которых связана с получением и обработкой ПДн, дают письменное обязательство о неразглашении ПДн, оформленное в виде дополнительного соглашения к трудовым договорам;
- со всеми принимаемыми на работу работниками, деятельность которых будет связана с обработкой ПДн, заключаются трудовые договоры и подписываются соответствующие должностные инструкции, в которых должны быть отражены вопросы обязанности обеспечения конфиденциальности ПДн (положения, подлежащие включению в трудовые договора и должностные инструкции работников приведены в приложении Г;
- в договоры со всеми физическими или юридическими лицами, которым Оператор поручает обработку ПДн, включаются положения, предусматривающие обязанность обеспечения указанными лицами конфиденциальности и безопасности ПДн при их обработке;
- осуществляется разделение полномочий пользователей в ИСПДн Оператора в зависимости от их должностных обязанностей;
- наличие формализованной процедуры по предоставлению доступа к ИСПДн, а также по регулярному пересмотру прав доступа работников в зависимости от занимаемой ими должности.

Оператор передает ПДн на обработку третьим лицам, только если это необходимо для достижения целей обработки ПДн, причем существенным условием договора является обязанность обеспечения третьей стороной конфиденциальности ПДн и безопасности ПДн при их обработке.

Передача ПДн третьим лицам без заключенного договора и без применения мер защиты ПДн не осуществляется.

Работа с ПДн, осуществляемая без использования средств автоматизации

ПДн при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных данных (далее – материальные носители), в специальных разделах или на полях форм (бланков).

При фиксации ПДн на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

Работники, осуществляющие обработку ПДн без использования средств автоматизации, до начала обработки информируются Ответственным за организацию обработки ПДн о факте обработке ими ПДн, о категориях ПДн, об особенностях и правилах обработки ПДн.

В типовую форму, в которую происходит внесение ПДн, включается следующая информация:

- цель обработки ПДн, наименование и адрес Оператора, источник получения ПДн, срок обработки ПДн, перечень действий с ПДн, которые будут совершаться в процессе их обработки;
- поле для проставления субъектом ПДн отметки о согласии на обработку ПДн без использования средств автоматизации.

Типовая форма должна быть составлена таким образом, чтобы каждый из субъектов ПДн, содержащихся в документе, имел возможность ознакомиться со своими ПДн, содержащимися в документе, не нарушая прав и законных интересов иных субъектов ПДн.

При несовместимости целей обработки ПДн, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку ПДн, принимаются меры по обеспечению раздельной обработки ПДн, в частности:

- при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других ПДн осуществляется копирование ПДн, подлежащих распространению или использованию, способом, исключающим одновременное копирование ПДн, не подлежащих распространению и использованию, и используется (распространяется) копия ПДн;
- при необходимости уничтожения или блокирования части ПДн уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование ПДн, подлежащих уничтожению или блокированию.

Уничтожение или обезличивание части ПДн, если это допускается материальным носителем, производится способом, исключающим дальнейшую обработку этих ПДн с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

Уточнение ПДн при осуществлении их обработки без использования средств автоматизации производится путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными ПДн.

Обработка ПДн, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории ПДн можно было определить места хранения ПДн (материальных носителей) и установить перечень лиц, осуществляющих обработку ПДн либо имеющих к ним доступ.

Оператор осуществляет раздельное хранение ПДн (материальных носителей), обработка которых осуществляется в различных целях.

Материальные носители с ПДн не оставляются без присмотра. Лица, ответственные за носители ПДн, при покидании рабочего места должны убирать носители ПДн в сейф или шкаф, закрывающийся на ключ. Кабинеты, в которых хранятся документы, содержащие ПДн, при покидании их работниками запираются.

Взаимодействие с государственными органами

Оператор сообщает в уполномоченный орган по защите прав субъектов ПДн по его запросу информацию, необходимую для осуществления деятельности указанного органа, в течение тридцати дней с даты получения запроса.

В случае получения запроса или обращения уполномоченного органа по защите прав субъектов ПДн о недостоверности ПДн или неправомерных действиях с ними выявленные нарушения подлежат исправлению. Оператор сообщает в указанный орган об устранении нарушений либо об уничтожении ПДн в случае невозможности устранения нарушений в срок, в течение десяти рабочих дней.

В установленных федеральным законодательством случаях Оператор предоставляет информацию, содержащую обрабатываемые ПДн, по мотивированному запросу уполномоченных органов государственной власти по вопросам их компетенции.

Запросы на предоставление доступа к обрабатываемым ПДн могут быть обжалованы в судебном порядке в соответствии с законодательством Российской Федерации.

Организация доступа к ПДн

Ответственным за обработку ПДн разрабатывается Перечень должностей работников, допущенных к работе с ПДн, определяющий связь между должностями работников и ПДн, к которым предоставляется доступ. Этот перечень подлежит пересмотру и при необходимости актуализации не реже одного раза в год.

Работникам Оператора предоставляется доступ к работе с ПДн исключительно в пределах и объеме, необходимых для выполнения ими своих должностных обязанностей.

Доступ к ПДн может быть прекращен или ограничен в случае нарушения требований настоящего Положения либо в случае изменения должностных обязанностей или увольнения работника.

Предоставление и прекращение доступа пользователей к ПДн осуществляется Администраторами соответствующей ИСПДн.

Требования к работникам, допущенным к обработке персональных данных

Все работники Оператора, которым стали известны ПДн, обрабатывающиеся Оператором, должны обеспечивать их конфиденциальность.

Все работники Оператора, допущенные к работе с ПДн, должны быть ознакомлены под подпись с требованиями настоящего Положения.

Оператором должен быть организован процесс обучения работников, допущенных к работе с ПДн, по направлению обеспечения безопасности ПДн. Ответственность за процесс обучения возлагается на Ответственного за организацию обработки ПДн.

Трудовые договора (или должностные инструкции) работников, допущенных к работе с ПДн, содержат раздел, описывающий персональную ответственность за нарушение требований по обеспечению безопасности ПДн, включая нарушение свойств целостности, конфиденциальности, доступности и установленного порядка обработки ПДн.

В случае нарушения установленного порядка обработки ПДн работники Оператора несут ответственность в соответствии с разделом 8 настоящего Положения.

Ответственность за нарушения при обработке ПДн

Работники Оператора несут персональную ответственность за соблюдение требований по обработке и обеспечению безопасности ПДн, установленных настоящим Положением, в соответствии с законодательством Российской Федерации.

Работник Оператора может быть привлечен к ответственности в случаях:

- умышленного или неосторожного раскрытия ПДн;
- утраты материальных носителей ПДн;
- нарушения требований настоящего Положения и других локальных нормативных актов Оператора по вопросам обработки и защиты ПДн.

В случае нарушения установленного порядка обработки и обеспечения безопасности ПДн, несанкционированного доступа к ПДн, раскрытия ПДн и нанесения Оператору, его работникам, клиентам и другим субъектам ПДн материального или иного ущерба виновные лица несут предусмотренную законодательством Российской Федерации ответственность.

Адекватную защиту персональных данных обеспечивают страны, подписавшие и ратифицировавшие Конвенцию Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, а также иные иностранные государства, обеспечивающих адекватную защиту прав субъектов персональных данных в соответствии с ФЗ «О персональных данных».