

УТВЕРЖДАЮ
Генеральный директор
А.В. Покатилов
«23» ноября 2022 г.

**Положение об обработке и обеспечении безопасности
персональных данных физических лиц
ООО «Интернет-Технологии»**

г. Ярославль
2022 год

1. Общие положения

1.1. Положение об обработке и обеспечении безопасности персональных данных физических лиц ООО «Интернет-Технологии» (далее – Организация, Оператор) разработано в соответствии с Конституцией РФ, Гражданским кодексом РФ, Трудовым кодексом РФ, ФЗ от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации», ФЗ от 27.07.2006 №152-ФЗ «О персональных данных», Постановлением Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляющейся без использования средств автоматизации», Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», Приказом ФСБ России от 10.07.2014 № 378 «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 РФ требований к защите персональных данных для каждого из уровней защищенности».

1.2. Положение разработано в целях обеспечения защиты прав и свобод физических лиц при обработке Организацией их персональных данных, определения порядка, принципов и целей обработки персональных данных физических лиц, категорий субъектов, персональные данные которых обрабатываются, категорий обрабатываемых персональных данных, установления мер по обеспечению безопасности персональных данных при их обработке.

2. Термины и определения

В Положении используются следующие основные термины и определения:

2.1. Оператор персональных данных – лицо, организующее и (или) осуществляющее обработку персональных данных, а также определяющее цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными. Оператором персональных данных в отношениях, регулируемых Положением, является Организация;

2.2. Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

2.3. Общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности;

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

3. Цели обработки персональных данных и категории субъектов, персональные данные которых обрабатываются

3.1. Организация является Оператором персональных данных в связи с обработкой персональных данных следующих категорий субъектов в рамках отношений, регулируемых Положением:

3.1.1. Лица, претендующие на трудоустройство или вступившие в трудовые отношения с Организацией, а также лица, прекратившие трудовые отношения с Организацией;

3.1.2. Представители лиц, с которыми Организация вступает в гражданско-правовые отношения;

3.1.3. Пользователи сервисов Организации и лица, состоящие с данными пользователями в трудовых и гражданско-правовых отношениях.

3.2. Организация обрабатывает персональные данные в отношении лиц, указанных в п. 3.1 Положения, в целях, определенных Трудовым кодексом РФ, а также иными нормами действующего законодательства РФ.

4. Принципы обработки персональных данных

4.1. Организация обрабатывает персональные данные на законной и справедливой основе.

4.2. Организация обрабатывает персональные данные лишь в целях, для которых они сообщены, и обеспечивает конфиденциальность полученных персональных данных, за исключением случаев, когда обеспечения конфиденциальности персональных данных не требуется: в случае обезличивания персональных данных и в отношении общедоступных персональных данных.

4.3. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки.

4.4. При обработке персональных данных обеспечиваются точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных.

5. Категории обрабатываемых персональных данных

5.1. Организация осуществляет обработку персональных данных, полученных непосредственно от субъекта персональных данных (его представителя), от третьих лиц, а также содержащихся в общедоступных источниках.

5.2. Организация обрабатывает следующие категории персональных данных в отношении лиц, указанных в п. 3.1.1 Положения:

- табельный номер;
- фамилия, имя, отчество;
- дата рождения (день, месяц, год рождения);
- паспортные данные (данные иного документа, удостоверяющего личность);
- пол;
- гражданство;
- личная фотография;
- состав семьи (в том числе количество детей);
- состояние в браке;
- идентификационный номер налогоплательщика;
- страховой номер индивидуального лицевого счета;
- адрес места жительства (адрес регистрации и фактический)
- код субъекта в соответствии с Классификатором адресов РФ;
- адрес электронной почты;
- номер телефона;
- сведения о воинском учете;
- сведения об образовании и квалификации (в том числе сведения о повышении квалификации, профессиональной переподготовке, аттестации, сведения о знании иностранного языка);
 - сведения о трудовой функции (должности, профессии, специальности, квалификации);

- условия и расчет оплаты труда (в том числе отпуска и иных выплат);
- сведения о работе (в том числе стаж работы, прежнее место работы, новое место работы, сведения о приеме на работу, сведения об увольнении с работы, сведения о переводе на другую работу);
 - сведения об учете рабочего времени;
 - сведения о награждении, почетных званиях и поощрении работника;
 - сведения о социальных льготах;
 - сведения о периоде отпуска;
 - сведения о структурном подразделении;
 - банковские реквизиты;
 - иные сведения, в случае если такие сведения предоставлены субъектами персональных данных в целях, определенных действующим законодательством и Положением.

5.3. Организация обрабатывает следующие категории персональных данных в отношении лиц, указанных в пункте 3.1.2 Положения:

- фамилия, имя, отчество;
- адрес места жительства (адрес регистрации и фактический)
- адрес электронной почты;
- номер телефона;
- иные сведения, в случае если такие сведения предоставлены субъектами персональных данных в целях, определенных действующим законодательством и Положением.

5.4. В соответствии с Политикой конфиденциальности Организация обрабатывает следующие категории персональных данных в отношении лиц, указанных в пункте 3.1.3 Положения:

- персональная информация, предоставленная лицами при регистрации (создании учетной записи): имя, номер телефона, адрес;
- электронные данные (HTTP-заголовки, IP-адрес, файлы cookie, веб-маяки/пиксельные теги, данные об идентификаторе браузера);
- дата и время осуществления доступа к сайтам и/или сервисам;
- информация об активности лиц во время использования сайтов и/или сервисов (например, история поисковых запросов; адреса электронной почты тех, с кем лица ведут переписку; содержание электронной почты и вложения, а также файлы, хранящиеся в системах Организации);
- информация о геолокации;
- иные сведения о лицах, необходимые для обработки в соответствии с условиями, регулирующими использование конкретных сайтов или сервисов Организации.

6. Обработка персональных данных

6.1. Обработка персональных данных осуществляется Организацией как с использованием средств автоматизации, так и без использования таких средств (смешанная обработка).

6.2. Право на обработку персональных данных лиц, состоящих в трудовых отношениях с Организацией, предоставляется работникам Организации при условии их ознакомления с Положением и включения таких лиц в Перечень лиц, доступ которых к персональным данным работников, обрабатываемым Организацией, необходим для выполнения ими обязанностей (Приложение №1).

6.3. Право на обработку персональных данных представителей лиц, с которыми Организация вступает в гражданско-правовые отношения, предоставляется работникам Организации при условии их ознакомления с Положением и включения таких лиц в Перечень лиц, доступ которых к персональным данным представителей лиц, с которыми

Организация вступает в гражданско-правовые отношения, необходим для выполнения ими обязанностей (Приложение №2).

6.4. Право на обработку персональных данных пользователей сервисов Организации и лиц, состоящих с такими пользователями в трудовых и гражданско-правовых отношениях, предоставляется работникам Организации при условии их ознакомления с Положением и включения таких лиц в Перечень лиц, доступ которых к персональным данным пользователей сервисов Организации, необходим для выполнения ими обязанностей (Приложение №3).

6.5. Право на обработку персональных данных в базах данных сервисов Организации предоставляется работникам Организации при условии их ознакомления с Положением и включения таких лиц в Перечень лиц, доступ которых к персональным данным в базах данных сервисов Организации, необходим для выполнения ими обязанностей (Приложение №4).

6.6. Основанием для исключения из перечней (Приложение №1, Приложение №2, Приложение №3, Приложение №4) работников Организации является приказ о прекращении трудового договора с работником.

6.7. При передаче персональных данных должен соблюдаться режим конфиденциальности информации.

6.8. Передача персональных данных в пределах Организации осуществляется с соблюдением требований, установленных Положением, и только лицам, уполномоченным на обработку персональных данных, в объеме, необходимом для совершения определенного действия (операции).

6.9. Передача персональных данных представителю субъекта персональных данных осуществляется в объеме, соответствующем объему его полномочий и необходимом для их исполнения.

6.10. Согласие на обработку персональных данных является основанием для их обработки, кроме случаев, предусмотренных законодательством. Согласие должно отвечать требованиям, предъявляемым к нему законодательством. В случае если в соответствии с требованиями федерального закона обработка персональных данных осуществляется с письменного согласия субъекта персональных данных, документ, содержащий согласие субъекта персональных данных, может быть составлен по форме, установленной Приложением №5 к Положению, или в произвольной форме, но с обязательным включением в него указанных в ч. 4 ст. 9 Федерального закона «О персональных данных» данных. Согласие на распространение персональных данных оформляется отдельно от иных согласий на обработку персональных данных (Приложение №6).

6.11. При передаче персональных данных Организация соблюдает следующие требования:

6.11.1. Не сообщать персональные данные третьей стороне без согласия субъекта персональных данных, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в случаях, установленных федеральным законом и Положением;

6.11.2. Предупреждать лиц, получивших персональные данные, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены. Лица, получившие персональные данные, обязаны соблюдать режим секретности (конфиденциальности);

6.11.3. Передавать персональные данные представителям субъекта персональных данных в порядке, установленном законодательством РФ, и ограничивать эту информацию только теми персональными данными, которые необходимы для осуществления указанными представителями их полномочий.

7. Меры по обеспечению безопасности персональных данных при их обработке. Хранение персональных данных

7.1. Хранение персональных данных, содержащихся как на бумажных, так и на электронных носителях, осуществляется в помещениях Организации. Персональные данные, содержащиеся на бумажном (электронном) носителе, могут быть воспроизведены соответственно на электронном (бумажном) носителе.

7.2. Организация при обработке персональных данных принимает необходимые организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий, с учетом требований, устанавливаемых действующим законодательством.

7.3. Обработка персональных данных осуществляется таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных.

7.4. Организацией применяются следующие необходимые и достаточные меры, направленные на обеспечение безопасности персональных данных:

- назначение Генеральным директором ответственных за организацию обработки персональных данных;
- организация режима обеспечения безопасности помещений, в которых осуществляется хранение персональных данных, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;
- контроль и управление физическим доступом к техническим средствам, а также в помещения и сооружения, в которых осуществляется хранение персональных данных, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации, в помещения и сооружения;
- обеспечение восстановления персональных данных, уничтоженных или измененных вследствие несанкционированного доступа к ним либо при отсутствии к тому основания;
- определение мест, в которых осуществляется обработка персональных данных;
- оценка эффективности принимаемых мер по обеспечению безопасности персональных данных при их обработке;
- ознакомление работников, уполномоченных на обработку персональных данных, с положениями нормативных правовых актов, регламентирующих обработку персональных данных;
- определение угроз безопасности персональных данных при их обработке;
- обнаружение фактов несанкционированного доступа к персональным данным;
- контроль за принимаемыми мерами безопасности персональных данных;
- соблюдение условий, обеспечивающих сохранность персональных данных и исключающих несанкционированный к ним доступ при хранении носителей персональных данных.

7.5. В состав мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных Организации с учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий, помимо мер, перечисленных в п. 7.4 Положения, входят:

- идентификация и аутентификация пользователей, являющихся работниками Организации; управление идентификаторами, управление средствами аутентификации; защита обратной связи при вводе аутентификационной информации; идентификация и аутентификация внешних пользователей;
- управление учетными записями пользователей; реализация необходимых методов, типов и правил разграничения доступа; управление информационными потоками

между устройствами, сегментами информационной системы; разделение полномочий пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы; назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы; ограничение неуспешных попыток доступа к информационной системе; реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети; регламентация и контроль использования в информационной системе технологий беспроводного доступа; регламентация и контроль использования в системе мобильных технических средств; управление взаимодействием с внешними информационными системами;

- регистрация событий безопасности, в том числе определение событий безопасности, подлежащих регистрации, и сроков их хранения; определение состава и содержания информации о событиях безопасности, подлежащих регистрации; сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения; защита информации о событиях безопасности;

- реализация антивирусной защиты; обновление базы данных признаков вредоносных компьютерных программ (вирусов);

- контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации;

- идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации; управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин;

- размещение устройств вывода информации, исключающее ее несанкционированный просмотр;

- обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи;

- обеспечение целостности информационной системы и персональных данных;

- обеспечение доступности персональных данных;

- управление конфигурацией информационной системы и системы защиты персональных данных.

7.6. Хранение и использование персональных данных осуществляется в соответствии со следующими требованиями и условиями:

7.6.1. Персональные данные обрабатываются и хранятся в помещениях Организации;

7.6.2. Персональные данные могут быть получены, проходить дальнейшую обработку и передаваться на хранение как на бумажных носителях, так и в электронном виде – локальной компьютерной сети и компьютерной программе;

7.6.3. Персональные данные передаются иным лицам в соответствии с целями, установленными действующим законодательством и Положением.

Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено действующим законодательством.

8. Ответственность за неправомерные действия с персональными данными

8.1. Совершенные работниками Организации действия (бездействие) с персональными данными, нарушающие требования нормативных правовых актов, Положения, иных локальных и других правовых актов Организации, являются основанием для привлечения совершивших такие действия (бездействие) лиц к дисциплинарной и (или) материальной ответственности.

8.2. Размер материальной ответственности ограничивается размером среднего месячного заработка, за исключением случаев, предусмотренных трудовым законодательством.

В частности, работник Организации несет полную материальную ответственность, если за предусмотренные п. 8.1 Положения действия (бездействие) он был привлечен к административной ответственности, установленной ст. 13.11 КоАП РФ «Нарушение законодательства Российской Федерации в области персональных данных» либо иными нормами законодательства об административных правонарушениях, или освобожден от такой ответственности в связи с малозначительностью совершенного нарушения.

8.3. Работник Организации подлежит привлечению к дисциплинарной и (или) материальной ответственности независимо от факта наличия (отсутствия) положений о возможности привлечения его к ответственности в трудовом договоре, должностной инструкции и иных документах, регламентирующих исполнение работником трудовой функции.

9. Заключительные положения

9.1. Положение вступает в силу с момента его утверждения и действует бессрочно до внесения соответствующих изменений или отмены действия Положения.

9.2. Изменения в Положение вносятся приказом Генерального директора Организации.

9.3. Положение применяется в отношении лиц, указанных в п. 3.1.3 Положения, поскольку это не противоречит Политике конфиденциальности Организации.