

Утверждено
Директором ООО «НОВОБЫТ-Р»
Приказ № 4
от 11 июля 2016г

Положение
«Об утверждении политики о защите персональных данных
используемой ООО «НОВОБЫТ-Р»

1. Общие положения

1.1. Настоящее Положение «Об утверждении политики о защите персональных данных используемой ООО «НОВОБЫТ-Р» (далее - Политика) разработана на основании:

1.1.1. Федерального закона № 152 «О защите персональных данных» от 27.07.2006г.

1.1.2. Постановления Правительства РФ № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» от 15.09.2008г.

1.1.3. Постановления Правительства РФ № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 01.11.2012г.

1.1.4. Иных нормативно-правовых актов РФ.

1.2. Целями настоящей Политики являются определение обработки и обеспечения безопасности персональных данных.

1.3. Настоящая Политика распространяется на все бизнес процессы ООО «НОВОБЫТ-Р», далее по тексту «Компания», и обязательна к выполнению всеми сотрудниками Компании.

1.4. В связи с общедоступностью настоящей Политики, более детальное описание процессов обработки и обеспечения безопасности персональных данных описано во внутренних нормативных документах.

1.5. Указанная политика предназначена для декларирования подхода Компании к обеспечению информационной безопасности. Размещается на сайте Компании в сети интернет для свободного доступа для любого пользователя, кто пожелает с ней ознакомиться.

2. Определения

1) персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

2) 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;

3) 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;

4) автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники;

5) распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

6) предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

7) блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

8) уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

9) обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

10) информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

11) Машинный носитель - магнитный диск, магнитная лента, лазерный диск и иные материальные носители, используемые для записи и хранения информации с помощью электронно-вычислительной техники.

3. Сокращения

ИБ - информационная безопасность

ИСПДн - информационная система персональных данных

НСД - несанкционированный доступ

ПДн - персональные данные

4. Принципы обработки и обеспечения безопасности персональных данных

4.1. Принципы обработки ПДн в Компани:

4.1.1. Обработка ПДн должна осуществляться на законной и справедливой основе.

4.1.2. Обработка ПДн должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка ПДн, несовместимая с целями сбора ПДн.

4.1.3. Обработке подлежат только ПДн, которые отвечают целям их обработки.

4.1.4. Содержание и объем обрабатываемых ПДн должны соответствовать заявленным целям обработки. Обрабатываемые ПДн не должны быть избыточными по отношению к заявленным целям их обработки.

4.1.5. При обработке ПДн должны быть обеспечены точность ПДн, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки ПДн. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.

4.1.6. Хранение ПДн должно осуществляться 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. Обрабатываемые ПДн подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

4.2. Компания как оператор, осуществляет обработку ПДн физических лиц в рамках требований законодательства РФ в целях:

4.2.1. Организации кадрового учета Компании, обеспечения соблюдения законов и иных нормативно-правовых актов, заключения и исполнения обязательств по трудовым и гражданско-правовым договорам; ведения кадрового делопроизводства, содействия работникам в трудоустройстве, обучении и продвижении по службе, пользования различного вида льготами, исполнения требований налогового законодательства в связи с исчислением и уплатой налога на доходы физических лиц, пенсионного законодательства, заполнения первичной статистической документации, в соответствии с Трудовым кодексом РФ, Налоговым кодексом РФ, федеральными законами, в частности: «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования».

4.2.2. Многократного пропуска субъектов ПДн на территорию Компании.

4.2.3. Заключение, исполнения и прекращения гражданско-правовых договоров с физическими, юридическими лицами, индивидуальными предпринимателями и иными лицами, в случаях, предусмотренных действующим законодательством РФ.

4.2.4. Предоставление физическим лицам разнообразных услуг, требующих осуществлять сбор и обработку ПДн.

4.3. В Компании используется смешанная обработка ПДн. Под смешанной обработкой понимается автоматизированная и неавтоматизированная обработка ПДн.

4.4. В случае достижения целей обработки ПДн, если другое не предусмотрено законодательством РФ, Компания прекращает обработку и производит уничтожение ПДн. Уничтожение ПДн, в электронном виде, и ПДн, содержащихся на материальных носителях, производится ответственными за этот процесс лицами согласно внутренней документации Компании.

4.5. В Компании используются современные и безопасные технологические решения для автоматизированной обработки, передачи и хранения персональных данных, исключающих несанкционированный доступ и утечку.

5. Основные требования к обработке ПДн

5.1. Обработка ПДн в Компании должна осуществляться с согласия субъекта ПДн, кроме случаев, когда такое согласие не требуется или же по поручению, в тех случаях когда Компания не является оператором ПДн субъектов.

5.2. В случаях, предусмотренных законодательством РФ, обработка ПДн осуществляется с согласия субъекта ПДн, оформляемого в соответствии со статьей 9 ФЗ №152.

5.3. Рекомендации к порядку получения согласия субъекта ПДн и виду согласия описаны во внутренней документации Компании.

5.4. В Компании ведется учет работников, допущенных к обработке ПДн. Учет ведется в согласованном Перечне лиц, допущенных к обработке ПДн.

5.5. Во избежание НСД к ПДн рекомендуется:

5.5.1. При неавтоматизированной обработке руководствоваться требованиями, предъявляемыми постановлением Правительства РФ №687 «Об утверждении положения об особенностях обработки ПДн, осуществляемой без использования средств автоматизации» от 15.09.2008г.

5.5.2. При автоматизированной обработке руководствоваться требованиями, предъявляемыми Постановлением Правительства РФ № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 01.11.2012г. и Приказом ФСТЭК России от 18.02.2013 N 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

6. Мероприятия по обеспечению безопасности ПДн

6.1. В состав мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных с учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий, входят:

- идентификация и аутентификация субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные (далее - машинные носители персональных данных);
- регистрация событий безопасности;
- антивирусная защита;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности персональных данных;
- обеспечение целостности информационной системы и персональных данных;
- обеспечение доступности персональных данных;
- защита среды виртуализации;

- защита технических средств;
- защита информационной системы, ее средств, систем связи и передачи данных;
- выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных (далее - инциденты), и реагирование на них;
- управление конфигурацией информационной системы и системы защиты персональных данных.

7. Права субъектов ПДн

7.1.Субъект ПДн согласно ФЗ имеет следующие права:

7.1.1.Субъект ПДн имеет право на получение информации, касающейся обработки его ПДн.

7.1.2.Субъект ПДн вправе требовать от оператора уточнения его ПДн, 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.

7.1.3.Сведения, предоставляются субъекту ПДн на основании запроса. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта ПДн или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта ПДн в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки ПДн оператором, подпись субъекта ПДн или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

8. Обязанности сотрудников Компании

8.1.Работники Компании, допущенные к обработке ПДн, обязаны:

8.1.1.Ознакомиться с данной Политикой и внутренними документами, регламентирующими процесс обработки ПДн, и выполнять требования этих документов.

8.1.2.Обрабатывать ПДн только в рамках выполнения своих должностных обязанностей.

8.1.3.Не разглашать ПДн, к которым был получен доступ в рамках исполнения своих трудовых обязанностей

8.1.4.Информировать о фактах разглашения (уничтожения, искажения) ПДн сотрудников, на которых возложены обязанности по ИБ.

9. Подразделение ответственное за контроль соблюдения Политики

9.1.Контроль обеспечения безопасности ПДн и соблюдения требований настоящей Политики осуществляется сотрудниками, на которых возложены обязанности по ИБ.

9.2.Контроль осуществляется путем разрешения инцидентов ИБ согласно внутренним документам Компании, а также в рамках иных контрольных мероприятий.

10. Ответственность за несоблюдение Политики

10.1.Сотрудники Компании, допустившие несоблюдение настоящей Политики, повлекшее за собой разглашение, утрату или нарушение целостности ПДн несут ответственность в соответствии с действующим законодательством РФ.

11. Заключительное положение

11.1.Изменения в настоящую Политику могут быть внесены директором Компании.

11.2.Настоящая Политика обязательна для соблюдения всеми сотрудниками Компании.

11.3.Режим конфиденциальности ПДн снимается в случаях их обезличивания, если иное не определено законодательством РФ.