

Утверждаю
Генеральный директор ООО «ДИОТРОНИКА»
Дунчев А.Н.



ПОЛОЖЕНИЕ ОБ ОБРАБОТКЕ И ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Настоящее Положение является локальным нормативным актом ООО "ДИОТРОНИКА" (далее - Общество), принятым с учетом требований, в частности, гл. 14 Трудового кодекса РФ, Федерального закона от 27.07.2006 № 152-ФЗ "О персональных данных" (далее - Закон о персональных данных). Настоящее Положение определяет порядок обработки и защиты персональных данных в ООО "ДИОТРОНИКА" (далее - работодатель) с целью применения и исполнения законодательства в рамках трудовых и иных непосредственно связанных с ними отношений.

1. КАТЕГОРИИ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

Субъекты, персональные данные которых обрабатываются работодателем: соискатели работы, работники, члены их семей, бывшие работники, а также иные лица, персональные данные которых работодатель обязан обрабатывать в соответствии с законодательством (далее - работники).

2. КАТЕГОРИИ И ПЕРЕЧЕНЬ ОБРАБАТЫВАЕМЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ, ЦЕЛИ ОБРАБОТКИ

2.1. Персональные данные (далее - ПДн) - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу:

- фамилия, имя, отчество, дата и место рождения, пол, гражданство, адрес и другие паспортные данные, фотография;
- ИНН, СНИЛС, водительское удостоверение, заграничный паспорт, паспорт иностранного гражданина (и иные документы, удостоверяющие личность иностранных граждан) номер телефона, адрес электронной почты, аккаунты в мессенджерах;
- сведения, содержащиеся в разрешении на временное проживание, разрешении на временное проживание в целях получения образования (для иностранных граждан, временно проживающих в РФ), виде на жительство (для иностранных граждан, постоянно проживающих в РФ);
- профессия, сведения об образовании, владении иностранными языками, местах работы, в том числе о предыдущих;
- данные воинского учета;
- сведения о семейном положении и членах семьи, о месте их работы или учебы;
- доходы, данные банковских счетов и карт;
- сведения о состоянии здоровья, связанные с возможностью выполнения трудовой функции;
- иные сведения, связанные с профессиональной деятельностью работника, а также иные персональные данные, которые работник пожелал сообщить о себе и обработка которых соответствует цели обработки, предусмотренной п. 3.1 Положения.

2.2. Работодатель создает и/или хранит следующие документы, содержащие ПДн:

- трудовые договоры и дополнительные соглашения к ним, заявления;
- анкеты, тесты и другие результаты испытаний при приеме на работу;
- копии документов об образовании, о наличии специальных знаний, квалификации и ее повышении, а также материалы аттестации работников;
- копии документов воинского учета;
- личные карточки работников, личные дела, трудовые книжки или сведения о трудовой деятельности;
- приказы по кадрам;
- отчетные материалы по оценке качества и эффективности работника, служебные и докладные записки, касающиеся работника;
- медицинские заключения о состоянии здоровья;
- документы со сведениями о заработной плате, банковских счетах и банковских картах;
- материалы внутренних расследований (акты, докладные, протоколы и др.);
- экземпляры отчетов для государственных органов;
- иные документы, предусмотренные законодательством.

2.3. Источником получения ПДн работника является работник. Получение ПДн работника у третьих лиц допускается на основании и в порядке, установленных законодательством РФ.

2.4. Цели обработки ПДн работника - соблюдение требований законодательства РФ и предоставление сведений:

- кредитным организациям - для открытия счета, оформления банковской карты, перечисления зарплаты и других выплат;
- страховым организациям - для заключения договора добровольного страхования работника;
- организациям, которые проводят обучение, в том числе по охране труда, - для прохождения обучения;
- работникам ООО "ДИОТРОНИКА" и третьим лицам - для выполнения работником трудовой функции, участия в развитии ООО «ДИОТРОНИКА».

2.5. Общество не осуществляет обработку специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни, за исключением случаев, предусмотренных законодательством РФ.

3. ЛИЦА, ОТВЕТСТВЕННЫЕ ЗА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Приказом генерального директора назначается лицо, ответственное за организацию обработки ПДн (далее - ответственное лицо), а также утверждается перечень лиц, имеющих доступ к ПДн в пределах, необходимых для выполнения своих трудовых обязанностей.

3.2. Ответственное лицо:

- контролирует соблюдение мер по защите ПДн;
- оформляет с лицами, имеющими право доступа к ПДн, письменное обязательство о неразглашении ПДн;
- принимает необходимые меры по хранению, обновлению и изменению ПДн;
- принимает необходимые меры по уничтожению либо обезличиванию ПДн работников после достижения целей обработки или в случае неактуальности, если иное не предусмотрено законодательством РФ.

3.3. Лица, получившие доступ к ПДн работников, обязаны соблюдать режим конфиденциальности. Данное положение не распространяется на передачу ПДн работников в порядке, установленном законодательством РФ.

3.4. Все лица, получающие доступ к ПДн, подписывают обязательство о неразглашении ПДн.

4. СПОСОБЫ И СРОКИ ОБРАБОТКИ И ХРАНЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Обработка ПДн - любое действие, совершаемое с ПДн с использованием средств автоматизации или без них, включая сбор, запись, систематизацию, накопление, хранение, обновление, изменение, извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение. Сбор и дальнейшая обработка ПДн работника возможны только с его письменного согласия, за исключением случаев, предусмотренных законодательством РФ.

4.2. ПДн работников можно обрабатывать на бумажных носителях и в электронном виде. При обработке ПДн работодатель обязан соблюдать принципы, ограничения и требования, установленные законодательством РФ.

4.3. Документы, в том числе в электронной форме, содержащие ПДн, хранятся в течение срока, установленного законодательством РФ, а если он не установлен - срока, определенного приказом генерального директора. После истечения срока хранения документы подлежат уничтожению.

4.4. Документы на бумажных носителях хранятся в запирающихся на замок шкафах. Доступ к документам в электронном виде возможен только по уникальному логину и паролю.

Обработка персональных данных в Обществе осуществляется с согласия субъекта персональных данных на обработку его персональных данных, если иное не предусмотрено законодательством в области персональных данных.

4.5. Обработка персональных данных, разрешенных субъектом персональных данных для распространения, осуществляется с соблюдением запретов и условий, предусмотренных ст. 10.1 Закона о персональных данных.

4.6. Согласие на обработку таких персональных данных оформляется отдельно от других согласий на обработку персональных данных. Согласие предоставляется субъектом персональных данных лично либо в форме электронного документа, подписанного электронной подписью, с использованием информационной системы Роскомнадзора.

4.7. Обработка биометрических персональных данных допускается только при наличии письменного согласия субъекта персональных данных. Исключения составляют ситуации, предусмотренные ч. 2 ст. 11 Закона о персональных данных.

4.8. Общество не осуществляет трансграничную передачу персональных данных.

4.9. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных в Обществе осуществляются посредством:

- получения оригиналов документов либо их копий;
- копирования оригиналов документов;
- внесения сведений в учетные формы на бумажных и электронных носителях;
- создания документов, содержащих персональные данные, на бумажных и электронных носителях;
- внесения персональных данных в информационные системы персональных данных.

4.10. В Обществе используются следующие информационные системы:

- корпоративная электронная почта;
- система электронного документооборота;
- система контроля за удаленным доступом;
- информационный портал.

4.11. Передача (распространение, предоставление, доступ) персональных данных субъектов персональных данных осуществляется в случаях и в порядке, предусмотренных законодательством в области персональных данных и Положением.

5. ПЕРЕДАЧА ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. Передача ПДн третьим лицам допускается только с письменного согласия работника, за исключением случаев предупреждения угрозы жизни и здоровью работника или в иных случаях, предусмотренных законодательством РФ.

5.2. Не допускается получение и передача работодателем информации о состоянии здоровья работника, за исключением сведений, относящихся к возможности выполнения трудовой функции.

6. СРОКИ ОБРАБОТКИ И ХРАНЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ

6.1. Обработка персональных данных в Обществе прекращается в следующих случаях:

- при выявлении факта неправомерной обработки персональных данных. Срок прекращения обработки - в течение трех рабочих дней с даты выявления такого факта;
- при достижении целей их обработки (за некоторыми исключениями);
- по истечении срока действия или при отзыве субъектом персональных данных согласия на обработку его персональных данных (за некоторыми исключениями), если в соответствии с Законом о персональных данных их обработка допускается только с согласия;
- при обращении субъекта персональных данных к Обществу с требованием о прекращении обработки персональных данных (за исключением случаев, предусмотренных ч. 5.1 ст. 21 Закона о персональных данных). Срок прекращения обработки - не более 10 рабочих дней с даты получения требования (с возможностью продления не более чем на пять рабочих дней, если направлено уведомление о причинах продления).

6.2. Персональные данные хранятся в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки. Исключение - случаи, когда срок хранения персональных данных установлен федеральным законом, договором, стороной которого (выгодоприобретателем или поручителем по которому) является субъект персональных данных.

6.3. Персональные данные на бумажных носителях хранятся в Обществе в течение сроков хранения документов, для которых эти сроки предусмотрены законодательством об архивном деле в РФ.

6.4. Срок хранения персональных данных, обрабатываемых в информационных системах персональных данных, соответствует сроку хранения персональных данных на бумажных носителях.

6.5. При достижении целей обработки персональных данных или в случае утраты необходимости в достижении этих целей персональные данные уничтожаются либо обезличиваются. Исключение может предусматривать федеральный закон.

6.6. Незаконно полученные персональные данные или те, которые не являются необходимыми для цели обработки, уничтожаются в течение семи рабочих дней со дня представления субъектом персональных данных (его представителем) подтверждающих сведений.

6.7. Персональные данные, обработка которых прекращена из-за ее неправомерности и правомерность обработки которых невозможно обеспечить, уничтожаются в течение 10 рабочих дней с даты выявления факта неправомерной обработки.

6.8 Персональные данные уничтожаются ежегодно не позднее 31 января, если иной срок не предусмотрен настоящим Положением и нормами законодательства, либо договором, стороной которого (выгодоприобретателем или поручителем, по которому) является субъект персональных данных, иным соглашением между ним и Обществом либо если Общество не вправе обрабатывать персональные данные без согласия субъекта персональных данных на основаниях, предусмотренных федеральными законами.

6.9. Персональные данные уничтожаются (если их сохранение не требуется для целей обработки персональных данных) в течение 30 дней с даты поступления отзыва субъектом персональных данных согласия на их обработку. Иное может предусматривать договор, стороной которого (выгодоприобретателем или поручителем, по которому) является субъект персональных данных, иное соглашение между ним и Обществом. Кроме того, персональные данные уничтожаются в указанный срок, если Общество не вправе обрабатывать их без согласия субъекта персональных данных на основаниях, предусмотренных федеральными законами

6.10. Ответственное лицо, составляет опись документов, подлежащих уничтожению. Уничтожает документы комиссия, созданная приказом генерального директора. Об уничтожении документов комиссия составляет акт.

6.11. Бумажные документы уничтожают в шредере. Электронные документы удаляют с информационных носителей.

7. ПРАВА, ОБЯЗАННОСТИ И ОТВЕТСТВЕННОСТЬ РАБОТНИКОВ

7.1. Работник обязан предоставлять работодателю достоверные сведения о себе.

7.2. Работник имеет право на полную информацию о находящихся у работодателя своих ПДн и их обработке.

7.3. Право работника на доступ к его ПДн может быть ограничено в случаях, установленных законодательством РФ.

7.6. Лица, виновные в нарушении порядка обработки и хранения ПДн, несут ответственность в соответствии с законодательством РФ.

8. ОРГАНИЗАЦИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ.

8.1. Без письменного согласия субъекта персональных данных Общество не раскрывает третьим лицам и не распространяет персональные данные, если иное не предусмотрено федеральным законом.

8.1.1. Запрещено раскрывать и распространять персональные данные субъектов персональных данных по телефону.

8.2. С целью защиты персональных данных в Обществе приказами генерального директора назначаются (утверждаются):

- работник, ответственный за организацию обработки персональных данных;

- форма согласия на обработку персональных данных, форма согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения;
- иные локальные нормативные акты, принятые в соответствии с требованиями законодательства в области персональных данных.

8.3. Работники, которые занимают должности, предусматривающие обработку персональных данных, допускаются к ней после подписания обязательства об их неразглашении.

8.4. Материальные носители персональных данных хранятся в шкафах, запирающихся на ключ. Помещения Общества, в которых они размещаются, оборудуются запирающими устройствами.

8.5. Доступ к персональной информации, содержащейся в информационных системах Общества, осуществляется по индивидуальным паролям.

8.6. В Обществе используется сертифицированное антивирусное программное обеспечение с регулярно обновляемыми базами.

8.7. Работники Общества, обрабатывающие персональные данные, периодически проходят обучение требованиям законодательства в области персональных данных.

8.8. В Обществе проводятся внутренние расследования в следующих ситуациях:

- при неправомерной или случайной передаче (предоставлении, распространении, доступе) персональных данных, повлекшей нарушение прав субъектов персональных данных;
- в иных случаях, предусмотренных законодательством в области персональных данных.

8.9. Работник, ответственный за организацию обработки персональных данных, осуществляет внутренний контроль:

- за соблюдением работниками, уполномоченными на обработку персональных данных, требований законодательства в области персональных данных, локальных нормативных актов;
- соответствием указанных актов требованиям законодательства в области персональных данных.

8.10. Внутренний контроль проходит в виде внутренних проверок. Внутренние проверки осуществляются по решению работника, ответственного за организацию обработки персональных данных. Основанием для них служит информация о нарушении законодательства в области персональных данных, поступившая в устном или письменном виде.

8.10.1 По итогам внутренней проверки оформляется докладная записка на имя генерального директора. Если выявлены нарушения, в документе приводится перечень мероприятий по их устранению и соответствующие сроки.

8.10.2. Внутреннее расследование проводится, если выявлен факт неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных (далее - инцидент).

8.10.3. В случае инцидента Общество в течение 24 часов уведомляет Роскомнадзор:

- об инциденте;
- его предполагаемых причинах и вреде, причиненном правам субъекта (нескольким субъектам) персональных данных;
- принятых мерах по устранению последствий инцидента;

- представителе Общества, который уполномочен взаимодействовать с Роскомнадзором по вопросам, связанным с инцидентом.

8.10.4. В течение 72 часов Общество обязано сделать следующее:

- уведомить Роскомнадзор о результатах внутреннего расследования;
- предоставить сведения о лицах, действия которых стали причиной инцидента (при наличии).

8.11. В случае предоставления субъектом персональных данных (его представителем) подтвержденной информации о том, что персональные данные являются неполными, неточными или неактуальными, в них вносятся изменения в течение семи рабочих дней. Общество уведомляет в письменном виде субъекта персональных данных (его представителя) о внесенных изменениях и сообщает (по электронной почте) о них третьим лицам, которым были переданы персональные данные.

8.12. Общество уведомляет субъекта персональных данных (его представителя) об устранении нарушений в части неправомерной обработки персональных данных. Уведомляется также Роскомнадзор, если он направил обращение субъекта персональных данных (его представителя) либо сам сделал запрос.

8.13. В случае уничтожения персональных данных, незаконно полученных или не являющихся необходимыми для заявленной цели обработки, Общество уведомляет субъекта персональных данных (его представителя) о принятых мерах в письменном виде. Общество уведомляет по электронной почте также третьих лиц, которым были переданы такие персональные данные.