Предисловие

Под кадровым обеспечением системы управления персоналом понимается необходимый количественный и качественный состав работников кадровой службы организации.

Уровень кадровой работы в организации зависит от профессиональной компетентности специалистов кадровых служб.

Цель делопроизводственного обеспечения — организация работы с документами, обращающимися в системе управления персоналом.

Делопроизводство составляет полный цикл обработки и движения документов с момента их создания работниками кадровой службы (или получения ими) до завершения исполнения и передачи в другие подразделения.

Раздел 1. Современное кадровое делопроизводство в коммерческих организациях

Тема 1. Организация защиты персональных данных при ведении кадрового делопроизводства

Защита персональных данных[1] — комплекс мероприятий технического, организационного и организационно-технического характера, направленных на защиту сведений, относящихся к определенному или определяемому на основании такой информации физическому лицу.

О персональных данных в РФ информируют:

- Конституция России;
- Трудовой Кодекс РФ;
- Федеральный закон № 152-ФЗ «О персональных данных»;
- Кодекс об административных правонарушениях РФ;
- Уголовный кодекс РФ.

Конституция РФ гарантирует:

- что каждый гражданин имеет право на личную, семейную или профессиональную тайну;
- имеет право контролировать распространение информации об этом, пресекать это распространение.

Если же данные распространяются недобросовестно, то гражданин вправе рассчитывать на защиту чести и достоинства.

Трудовой кодекс РФ говорит о том, что сбор персональных данных работника кадровиком или руководителем может проводиться исключительно с ясными и адекватными целями.

В Федеральном законе № 152-ФЗ отмечена необходимость соблюдения полной безопасности данных, обозначены права, обязанности и ответственность граждан и операторов обработки.

КоАП РФ и УК РФ устанавливают ответственность за нарушение указанных норм.

Нормативные акты РФ по работе с персональными данными устанавливают два важных понятия, которые необходимо

[1] www.kdelo.ru

иметь в виду руководителю и ответственному сотруднику кадровой службы, чтобы не навлечь на себя и на организацию огромные штрафы и судебные иски.

1. Избыточность.

2. Целеполагание.

То есть работодатель имеет право собирать исключительно те данные, которые необходимы для осуществления трудового процесса, и только с целью поддержания этого процесса.

Персональными данными являются:

• фамилия, имя, отчество;

• дата, место рождения;

• биометрия — отпечатки пальцев, ДНК, радужная оболочка глаз, рост, вес, фотографии и видео с изображением человека, если его можно там идентифицировать;

• адрес регистрации или фактического жительства;

• семейное положение, состав семьи;

• биографические данные;

• профессиональная информация — образование, квалификация, должность, трудовой стаж, предыдущие места работы;

• сведения о доходах и имуществе;

• номера ИНН и СНИЛС;

• контакты — телефон, электронная почта;

• информация о воинской обязанности;

• медицинская информация и диагнозы.

До 1 марта 2021 г. в законе существовало понятие «общедоступные персональные данные».

Это понятие упразднено. Теперь это звучит так — «персональные данные, разрешенные субъектом для распространения».

То есть — никто не вправе распространять личную информацию о субъекте без его согласия на это. Более того, даже если сам субъект распространит свои персональные данные или они будут опубликованы в другом источнике, транслировать их можно только с его прямого согласия.

Работодатели обязаны обеспечить защиту персональных данных работников от неправомерного использования или утраты (п. 7 ч. 1 ст. 86 ТК РФ).

К документам на бумаге требования стандартные — закрывать шкафы, где храните документы, на ключ, ограничивать к ним доступ неуполномоченных лиц.

А вот к документам, которые храните на компьютерах, требования жесткие.

Они зависят от типа угроз безопасности персональных данных и уровня защиты персональных.

Штраф за то, что с документами что-то случится, например, их украдут, распространят или уничтожат с 27 марта 2021 г. увеличили до 100 000 рублей (ч. 6 ст. 13.11 КоАП РФ).

Поэтому важно установить систему защиты персональных данных так, чтобы обеспечить информационную защиту персональных данных от неправомерных действий.

Чтобы обеспечить защиту персональных данных в организациях, сначала определите тип угрозы (п. 6 Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства от 01.11.2012 № 1119).

Типы угроз[2]:

1. Возникает, когда к неправомерному использованию персональных данных, которые хранятся в информационной системе, могут привести скрытые функциональные возможности системного, то есть предустановленного программного обеспечения. Речь идет о программах, которые входят в состав операционной системы.

2. Связан со скрытыми возможностями прикладного программного обеспечения. То есть программ, которые устанавливаете на компьютер дополнительно к системным. Это, например, программы, которые вы используете для автоматизации кадрового учета.

3. Предполагает, что от программного обеспечения, как системного, так и прикладного, угроз нет.

Определить тип потенциальной опасности самостоятельно, чтобы адекватно выбрать меры для защиты персональных данных в информационных системах, непросто.

Поэтому госслужащие подсказывают — обращайтесь в специализированные организации, у которых есть лицензия на деятельность по технической защите конфиденциальной информации (п. 2 Состава и содержания организационных и технических мер по обеспечению безопасности персональных

[2] Делопроизводство в кадровой службе. Под ред. Кибанова А. Я. М.: Проспект, 2021.

данных при их обработке в информационных системах персональных данных, утвержденных приказом ФСТЭК от 18.02.2013 № 21).

От типа угрозы зависят требования к уровню защищенности персональных данных.

То есть если неверно определим тип угрозы, есть вероятность принять недостаточные меры для защиты персональных данных.

2021 г. при этом стал годом увеличения штрафов за нарушения в этой области.

Штрафы за персональные данные увеличили в 10 раз, и теперь они — до полумиллиона рублей за одно нарушение.

Защита персональных данных сотрудников строится путем определения требований к уровню защищенности персональных данных.

Всего уровней — четыре (п. 9–12 Требований, утвержденных постановлением Правительства от 01.11.2012 № 1119).

УЗ-1 устанавливается:

• если существуют угрозы I типа и информационная система работает со специальными, биометрическими или иными категориями ПД;

• если существуют угрозы II типа и информационная система работает со специальными категориями ПД свыше 100 тысяч граждан.

УЗ-2 устанавливается при угрозах типов:

• I и работе с общедоступными личными данными;

• II и работе с личными данными служащих оператора или при работе со специальной категорией ниже 100 тысяч человек;

• II и работе с использованием биометрических личных данных;

• II и обработке общедоступных личных данных при количестве от 100 тысяч человек (без персонала оператора);

• II и работе с другими видами ПД с количеством от 100 тысяч человек (без учета работников оператора);

• III и работе со специальной категорией более чем 100 тысяч человек (не считая персонала оператора).

УЗ-3 устанавливается при наличии угроз следующих типов:

• II, включая работу с ПД общедоступного характера с количеством людей до 100 тысяч человек;

• II с работой с другими категориями до 100 тысяч человек;

• III с обработкой специальных категорий до 100 тысяч человек;

• III с использованием биометрических ПД;

• III с работой с другими категориями, превышающими 100 тысяч человек (кроме персонала оператора).

УЗ-4 устанавливается при угрозах:

• III типа и работе с общедоступной информацией;

• III типа и обработке других категорий меньше 100 тысяч человек.

Требования к системе защиты персональных данных напрямую зависят от того, какой уровень защищенности определили исходя из типа угроз безопасности данных.

При всех четырех уровнях защищенности нужно соблюдать четыре общих требования к защите персональных данных сотрудников организации (п. 13–16 Требований, утвержденных постановлением Правительства от 01.11.2012 № 1119):

1. Обеспечить режим безопасности помещений, в которых размещаете информационную систему, чтобы туда не проникали посторонние.

2. Обеспечить сохранность носителей информации.

3. Утвердить перечень сотрудников, которых допустили к персональным данным коллег.

4. Использовать средства защиты информации, которые прошли оценку соответствия требованиям закона в области обеспечения безопасности информации, если потребуется нейтрализовать угрозы безопасности.

Шаг 1. Выпустить положение о персональных данных. Этого требуют и федеральный закон, и здравый смысл. В локальном акте нужно прописать все правила хранения и обработки данных.

Шаг 2. Утвердить положение. Для этого нужно выпустить соответствующий приказ с подписью руководителя и ознакомить с ним всех сотрудников. Работники должны расписаться в специальном журнале или ведомости.

Шаг 3. Назначить специалиста, ответственного за персональные данные.

Вероятнее всего, это будет сотрудник кадровой службы. Желательно, чтобы работа с персональными данными была

указана в его трудовом договоре. Если же договор уже составлен, можно выпустить дополнительное соглашение к нему. В том же приказе нужно установить сотрудников, которые будут иметь доступ к персональным данным. Все упомянутые лица должны подписать обязательство о неразглашении данных.

Шаг 4. Собрать со всех сотрудников письменные согласия на обработку персональных данных. В письменном согласии должны быть перечислены конкретные данные и цели их использования.

Шаг 5. Хранить данные в строгом порядке. Данные могут храниться и в электронном виде, и в бумажном. Они должны быть абсолютно недоступными для третьих лиц, своевременно пополняться и при необходимости корректироваться.

Шаг 6. Обратиться в Роскомнадзор.

Этот пункт не обязателен, если Вы:

• обрабатываете информацию без использования специализированного ПО и баз данных (то есть если массив данных оператор обрабатывает вручную на ПК или на бумаге);

• обрабатываете данные только своих сотрудников и только в целях составления и ведения трудовых договоров (не более);

• оформили договор с физическим лицом как подрядчиком, поставщиком или нештатным специалистом;

• однократно пропустили постороннего человека, не являющегося Вашим сотрудником, на территорию предприятия (например, для собеседования).

С 1 июля 2021 г.:

• Определен новый порядок прохождения инспекционных проверок, в том числе и Роскомнадзора. Вступил в силу Федеральный закон от 31.07.2020 № 248-ФЗ «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации».

• Определен новый порядок прохождения проверок органами Роскомнадзора, который введен в действие Постановлением Правительства РФ от 29.06.2021 № 1046 «О федеральном государственном контроле (надзоре) за обработкой персональных данных».

Оператор ПДн[3] — компания, которая собирает, хранит, обрабатывает и распространяет персональные данные.

[3] www.kdelo.ru

Чтобы понять, является ли компания оператором, нужно разобраться, что такое хранение и обработка персональных данных:

1. Хранение персональных данных по ФЗ № 152-ФЗ — это когда вы держите данные у себя, например, записали на свой сервер или в базу данных в облаке. Кстати, если данные на бумаге, и Вы держите их в папках и архивах, то тоже занимаетесь хранением персональных данных.

2. Обработка персональных данных — любые действия с ними: запись, извлечение, анализ, изменение, передача и даже удаление. Даже если Вы просто собираете данные, Вы их уже обрабатываете.

С 1 марта 2021 г. в организации нужно оформлять документ — согласие на распространение персональных данных (ст. 10.1 ФЗ № 152-ФЗ).

Требования к форме согласия установлены ст. 9 ФЗ № 152-ФЗ. Количество согласий на обработку персональных данных зависит от количества субъектов, чьи данные обрабатываются в организации.

В 2022 г. согласие работников на обработку личных сведений можно не брать в случае, если организация занимается обработкой этих данных и это прописано в трудовом договоре (п. 5 ч. 6 ФЗ № 152-ФЗ).

Работодателям необходимы данные сотрудников для начисления заработной платы, ведения кадровой документации и других видов отчетности.

Не требуется согласие работника на передачу персональных данных третьим лицам в целях предупреждения угрозы жизни и здоровью работника, в ФСС, ПФ РФ, налоговые органы, военные комиссариаты, прокуратуру, правоохранительные органы, ГИТ, суд (Разъяснения Роскомнадзора «Вопросы, касающиеся обработки персональных данных работников, соискателей на замещение вакантных должностей, а также лиц, находящихся в кадровом резерве»).

Закон РФ утверждает требования относительно содержания согласия на обработку данных человека, на которые дано его разрешение (Приказ Роскомнадзора № 18).

Согласие должно быть составлено письменно и содержать:

1) данные физического лица, дающего согласие, то есть:

• фамилия, имя, отчество;

• личный телефон;
• адрес;
• электронную почту;

2) данные организации, которая получает информацию о гражданине — ее наименование, юридический адрес, ЕГРЮЛ, ОГРН, ИНН;

3) цель для обработки сведений о физическом лице, к примеру, публикация данных на личном портале осуществляется для роста продаж и увеличения доверия клиентов;

4) группы и список данных, то есть человек обязан перечислить, какую именно информацию он разрешает или не разрешает обрабатывать;

5) период действия данного согласия, то есть временной интервал, когда действует настоящее согласие, дата начала и окончания;

6) название ресурса, где человек разрешает размещать личные данные с указанием конкретного раздела в случае, если сведения будут подвержены публикации.

Согласие на обработку персональных данных

Я, Иванов Петр Васильевич, паспорт серии 32 12, номер 634789, выдан 06.07.2013 УФМС России по Курской обл. в Курском районе, проживающий по адресу: г. Курск, просп. Дружбы, д. 33, в соответствии со ст. 9 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» даю согласие ООО «Ватрушка», расположенному по адресу: г. Курск, ул. Черняховского, д. 12, на обработку в документальной и (или) электронной форме моих персональных данных для оформления информационного стенда.

Перечень моих персональных данных, на обработку которых я даю согласие:
— фамилия, имя, отчество;
— фотография;
— пол;
— образование, квалификация, повышение квалификации;
— трудовая деятельность в ООО «Ватрушка».

Настоящее согласие действует в течение всего срока трудового договора.

Настоящее согласие может быть отозвано мной в письменной форме.

05.09.2018 П.В. Иванов

Если организация передает третьему лицу персональные данные работника не в рамках трудовых отношений (например, аудиторам для проверки), она обязана уведомить об этом Роскомнадзор по определенной форме ч. 1, 2 ст. 22 ФЗ № 152-ФЗ; Приложение № 1 к Приказу Роскомнадзора от 30.05.2017 № 94.

Уведомление подается на основании ч. 3 ст. 22 ФЗ № 152-ФЗ или в бумажном виде в адрес территориального органа Роскомнадзора, или в электронном виде через портал персональных данных.

Согласие на передачу персональных данных

Я, Иванов Петр Васильевич, паспорт серии 32 12, номер 634789, выдан 06.07.2013 УФМС России по Курской обл. в Курском районе, проживающий по адресу: г. Курск, просп. Дружбы, д. 33, в соответствии со ст. 9 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» даю согласие ООО «Ватрушка», расположенному по адресу: г. Курск, ул. Черняховского, д. 12, на передачу в ПАО «Банк»: фамилии, имени, отчества; должности; размера заработной платы.

Цель передачи и обработки: получение кредита.

Срок действия согласия: две недели, следующие за днем получения кредита.

10.10.2018 П.В. Иванов

Согласно изменению законодательства, в текущем году гражданин вправе в любой момент выдвинуть требование о прекращении обработки личных сведений, разрешение на которое было выдано им ранее (п. 12 ст. 10.1 ФЗ № 152-ФЗ).

В подобных ситуациях организация обязана прекратить распространение персональных данных немедленно, а действие согласия с этого момента прекращается.

Отказ гражданина должен быть оформлен в письменном виде, с указанием своих личных данных и списка той информации, передача которой должна быть прекращена.

Суды и другие правоохранительные органы могут беспрепятственно получать от компаний персональные данные сотрудников, клиентов или контрагентов без согласия последних.

Но ответ на вопрос о том, имеют ли аналогичные права другие контролирующие структуры и какие именно, приходится искать не только в законах, но и в судебной практике.

Пример, Девятый арбитражный апелляционный суд в своем Постановлении от 25.06.2009 по делу № А40-76345/08-122-112 указал, что сотрудник службы судебных приставов не имеет права запрашивать и получать сведения, содержащие личные данные граждан.

Суд отметил, что ни Федеральный закон от 21.07.1997 № 118-ФЗ «О судебных приставах», ни Федеральный закон от 02.01.2007 № 229-ФЗ «Об исполнительном производстве» не предоставляют судебным приставам-исполнителям права получать персональные данные без согласия их субъектов, не устанавливают условия получения таких данных, не определяют круг субъектов, персональные данные которых подлежат обработке, а также полномочия судебного пристава-исполнителя по их обработке.

Если Ваша организация осуществляет передачу персональных данных в другую страну, то возникает проблема защиты персональных данных при их трансграничных перемещениях.

Трансграничная передача данных[4] — это передача персональных данных оператором через государственную границу Российской Федерации органу власти, физическому или юридическому лицу иностранного государства.

В Российской Федерации одним из критериев оценки государства с точки зрения организации им адекватного уровня защиты может выступать факт ратификации им Конвенции о защите прав физических лиц при автоматизированной обработке персональных данных от 28.01.1981 ETS № 108.

До начала передачи оператор должен убедиться в том, что на территории иностранного государства обеспечена защита прав субъектов персональных данных.

Присоединение иностранного государства к Конвенции о защите физических лиц при автоматизированной обработке персональных данных (Страсбург, 1981 г.; с изменениями 1999 г.) позволяет причислять его к числу тех, кто гарантирует вполне адекватную защиту.

Режим конфиденциальности персональных данных снимается в случаях их обезличивания или по истечении 75-летнего срока их хранения, если иное не определено законом.

[4] www.kdelo.ru

Согласно ФЗ № 152-ФЗ, персональные данные должны быть уничтожены оператором по достижении цели их обработки.

Например, первичные документы по кадровому учету и заработной плате необходимо хранить в течение 75 лет. Но они должны находиться в архиве, а ФЗ № 152-ФЗ на архив не распространяется в соответствии с законом об архиве. Таким образом, после сдачи документов в архив организация уже не может хранить эти сведения у себя.

Что необходимо проверить:

1. Состоит ли организация в реестре Роскомнадзора как оператор, осуществляющий обработку персональных данных в соответствии с требованиями ст. 22 ФЗ № 152-ФЗ.

Для этого нужно: зайти на сайт Роскомнадзора, в разделе «Персональные данные» выбрать «Реестр операторов персональных данных» и указать в нем название организации, ИНН и регистрационный номер. Если поиск не дал результатов, регистрация отсутствует.

2. Есть ли в организации Политика в отношении персональных данных.

Если есть, проверьте, размещена ли она в открытом доступе на сайте организации. При отсутствии сайта для ознакомления с Политикой в организации к ней должен быть обеспечен неограниченный доступ.

Пример: Политику можно разместить перед входом в организацию на информационном стенде.

3. Со всеми ли соискателями, работниками и иными третьими лицами подписаны согласия на обработку персональных данных.

Если нет, необходимо получить эти согласия. При этом обязательно проверьте, соответствует ли форма согласия на обработку персональных данных требованиям п. 4 ст. 9 ФЗ № 152-ФЗ.

Пример: в согласии могут быть не указаны все третьи лица, которым передаются персональные данные. Или отсутствует перечень действий по персональным данным. Или некорректно указаны или вовсе не указаны условия обработки и распространения персональных данных.

4. Если в организации персональные данные субъектов распространяются в неограниченном кругу лиц, есть ли специ-

альные согласия на такое распространение. Это новое требование, которое вступило в силу с 1 марта 2021 г.

5. Всем ли работникам, в должностные обязанности которых входит работа с персональными данными, установлены разграничения по соответствующему доступу (полному или ограниченному). Необходимо оформить доступ: условия указать в локальном нормативном акте (например, Положении по персональным данным) либо приказах по организации, а также должностных инструкциях работников.

6. Назначено ли ответственное лицо или лица за организацию обработки персональных данных (ст. 18.1 и 22.1 ФЗ № 152-ФЗ).

7. Соответствуют ли используемые типовые формы документов (приказов, уведомлений, соглашений, графиков и т. д.) требованиям Постановления Правительства РФ от 15.09.2008 № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

В соответствии со ст. 23 ФЗ № 152-ФЗ для обеспечения контроля и надзора за соответствием обработки персональных данных требованиям Федерального закона назначается Уполномоченный орган по защите прав субъектов персональных данных.

Такие функции возложены на три учреждения:

• на Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) в части, касающейся соблюдения норм и требований по обработке персональных данных;

• на Федеральную службу безопасности РФ в части, касающейся соблюдения требований по организации и обеспечению функционирования шифровальных (криптографических) средств в случае их использования для обеспечения безопасности персональных данных при их обработке в ИСПДн;

• на Федеральную службу по техническому и экспортному контролю в части, касающейся контроля и выполнения требований по организации и техническому обеспечению безопасности ПДн (не криптографическими методами) при их обработке в ИСПДн.

В рамках своих полномочий регуляторы имеют право проводить плановые и внеплановые проверки.

Роскомнадзор проводит плановые проверки с целью контроля сведений, указанных в уведомлении уполномоченного органа по защите ПДн, а также внеплановые — на основании заявления физических лиц с целью проверки информации, указанной в данном заявлении.

ФСБ России имеет право проводить плановые проверки:

• представление по запросу отчета по лицензируемым видам деятельности;

• представление копий аттестатов соответствия по требованиям информационной безопасности на автоматизированные системы, в составе которых эксплуатируются системы криптографической защиты информации (СКЗИ);

• явочная проверка выполнения организационных мер на объектах лицензируемых видов деятельности.

ФСТЭК РФ уполномочен осуществлять плановые проверки:

• представление по запросу отчета по лицензируемым видам деятельности;

• представление копий аттестатов соответствия по требованиям информационной безопасности на автоматизированные системы;

• представление копий аттестатов соответствия на защищаемые помещения по требованиям безопасности;

• явочная проверка выполнения организационных мер на объектах лицензируемых видов деятельности.

Самые распространенные нарушения по персональным данным:

1) обработка персональных данных соискателя и третьих лиц без получения от них согласия в установленном порядке;

2) использование согласия на обработку персональных данных по форме, не соответствующей требованиям норм действующего законодательства;

3) отсутствие или не размещение Политики в отношении персональных данных на сайте организации либо необеспечение неограниченного доступа к данному документу в организации;

4) несоответствие локального нормативного акта по персональным данным требованиям норм действующего законодательства;

5) отсутствие в организации ответственного лица или лиц за организацию обработки персональных данных;

6) незаконная передача персональных данных третьим лицам (без согласий либо с согласиями, оформленными с нарушениями);

7) нарушение порядка хранения и уничтожения персональных данных в информационных системах и на бумажных носителях;

8) нарушение порядка предоставления персональных данных или документов, содержащих персональные данные работников.

Ответственность за неправильное или небезопасное хранение данных очень серьезная.

Если организация что-то сделает не так по ПДн, она навлечет на себя проверки, административное производство или уголовный процесс.

Административная ответственность. До 75 000 рублей штрафа работодатель может заплатить:

- за сбор и обработка избыточной информации;
- отсутствие согласия работника на обработку данных;
- доступ третьих лиц к персональным данным сотрудников;
- игнорирование просьб работника об удалении его персональных данных (например, после его увольнения).

Уголовная ответственность. По ст. 137 УК РФ: разглашение данных работника в публичном пространстве, публикация в СМИ сведений, составляющих его личную или семейную тайну. Штраф до 200 000 рублей, лишение свободы до 2 лет и запрет занимать определенные должности — до 3 лет.

То же самое, с использованием служебного положения — штраф до 300 000 рублей, лишение свободы до 5 лет и запрет занимать соответствующую должность — до 6 лет.

Регулярно отслеживайте изменения и своевременно вносите исправления в документы, корректируйте процессы по персональным данным, которые существуют в организации.

Следите за актуальностью локальных нормативных актов, согласий, приказов, инструкций, регламентов, типовых форм и другие документов, в которых содержатся персональные данные и к которым установлены требования законодательства по их оформлению.

Помните о соблюдении процессов обработки персональных данных.

При работе с персональными данными учитывайте обязательные требования норм действующего законодательства, которые несут наибольшие риски.

Обязательно сделайте чек-лист и проверьте по нему: состоите ли вы на учете в органах Роскомнадзора или нет, какие документы по персональным данным у вас оформлены с учетом их содержания, а какие нет, со всеми ли субъектами, чьи данные Вы обрабатываете, подписаны необходимые согласия, все ли процессы по передаче персональных данных налажены и защищены, есть ли ответственные лица за организацию обработки персональных данных.

Тема 2. Документирование приема на работу

Прием на работу оформляется трудовым договором. Работодатель вправе издать на основании заключенного трудового договора приказ (распоряжение) о приеме на работу. Содержание приказа (распоряжения) работодателя должно соответствовать условиям заключенного трудового договора.

По общему правилу работник имеет право быть принятым на работу, если он достиг возраста 16 лет.

Из этого правила существуют исключения:

1) на работу, связанную с химическим оружием, принимаются лица, достигшие возраста 20 лет;

2) с 18 лет принимаются:

- на работу иностранные граждане;
- на работу с вредными, опасными условиями труда;
- на подземные работы;
- на работы, где запрещен труд несовершеннолетних;
- на работу вахтовым методом;
- на работу в религиозную организацию;
- на работу в ночных кабаре и клубах, работы, связанные с производством, перевозкой и торговлей спиртными напитками, табачными изделиями, наркотическими препаратами, материалами эротического содержания, в игорный бизнес;
- на работы, связанные с подъемом и перемещением тяжестей выше установленных норм;
- на работу спасателем в профессиональные спасательные организации;

Конец ознакомительного фрагмента.
Приобрести книгу можно
в интернет-магазине
«Электронный универс»
e-Univers.ru