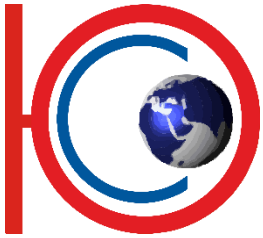
Центр дополнительного профессионального образования

«Южная Столица»



Методический материал

Кадровое делопроизводство

ТЕМА 5.

РАБОТА С ПЕРСОНАЛЬНЫМИ ДАННЫМИ

Тел.: ***8-918-121-20-20***

Эл.адрес: ***uq-city07@mail.ru***

Сайт: ***юс123.рф***

г. Краснодар

2020г.

Оглавление

1. Защита информации 2
1.1. Понятие персональных данных 2
1.1. Подбор персонала 6
2. Процесс защиты персональных данных в службе делопроизводства 7
2.1. Принципы защиты персональных данных работников 9
2.2. Особенности технологии защиты персональных данных 10
2.3. Особенности хранения документации 12
2.4. Размещение и организация работы кадровой службы 13
2.5. Регламентирующие документы службы делопроизводства 14
2.6. Работа с посетителями в кадровой службе 15
3. Ответственность за нарушение закона 152-ФЗ 17
4. Примерный образец Положения о защите персональных данных 20

1. Защита информации

Работа службы персонала, управления или отдела кадров, менеджера по персоналу, иногда, в некрупных фирмах, секретаря-референта неразрывно связана с накоплением, формированием, обработкой, хранением и использованием значительных объемов сведений о всех категориях сотрудников. Эти сведения относятся к так называемым персональным данным, которые по своей сути отражают личную или семейную тайну граждан, их частную жизнь и входят в круг информации, подлежащей защите от несанкционированного доступа.

1.1. Понятие персональных данных

Личная тайна гражданина охраняется Конституцией Российской Федерации. Разглашение этой тайны т. е. бесконтрольное распространение персональных данных во времени и пространстве, может нанести значительный ущерб физическому лицу. Понятие личной тайны близко примыкает к семейной тайне. Семейная тайна или тайна нескольких физических лиц, членов семьи не тождественна личной тайне по составу защищаемых сведений. Например, к семейной тайне относятся: тайна усыновления, тайна отцовства, тайна наследственного заболевания и др.

Согласно закону № 152-ФЗ, ***персональные данные*** – это любая информация, которая прямо или косвенно относится к определенному или определяемому физическому лицу. То есть о персональных данных можно говорить, если по информации или ее совокупности можно понять, о ком именно идет речь. Если же идентифицировать личность нельзя, то такие сведения нельзя отнести к персональным данным.

Персональные данные всегда относятся к категории конфиденциальной информации. Не допускаются сбор, передача, уничтожение, хранение, использование и распространение информации о частной жизни, а равно информации, нарушающей личную тайну, семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений физического лица без его согласия, кроме как на основании судебного решения. Режим конфиденциальности персональных данных снимается в случаях обезличивания этих данных или по истечении 75лет срока их хранения, если иное не определено законом.

Исчерпывающего списка персональных данных в законодательстве не приводится. Относятся данные к персональным или не относятся, решается в каждой ситуации отдельно. Но обычно к ним принято относить:

- ✓ фамилию, имя, отчество;
- ✓ адрес проживания;
- ✓ электронный адрес;
- ✓ номер телефона;
- ✓ дата рождения;
- ✓ место рождения;
- ✓ национальность;
- ✓ вероисповедание;
- ✓ место работы;
- ✓ должность;
- ✓ рост;

- ✓ вес;
- ✓ и т.д.

Аппараты, устройства, используемые для работы со сведениями персонального характера с участием человека, называются ***неавтоматизированными***. Они призваны обеспечить работу с информацией, ее хранение, уточнение, извлечение или уничтожение, при этом, не могут служить инструментами компьютеризации данных и не позволяют работать с большими массивами информации – операция со сведениями каждого субъекта ПД проводится отдельно и вручную оператором.

Определение обработки ПДн неавтоматизированного типа находим в Постановлении Правительства РФ от 15 сентября 2008 года № 678 «Об утверждении Положения об особенностях обработки ПДн, осуществляемой без использования инструментов автоматизации». В документе указано, под ручной работой с ведомостями подразумевается один из процессов, например, использование, уточнение, распространение, обезличивание или уничтожение информации при непосредственном участии человека.

Под ***автоматизированной*** обработкой персональных данных понимается их обработка при помощи средств вычислительной техники. Средствами вычислительной техники могут быть электронные вычислительные машины, комплексы и сети, вспомогательные и периферийные устройства, в том числе и установленное программное обеспечение. С автоматизированной обработкой персональных данных всё понятно, но вопрос о том, что же является неавтоматизированной обработкой остается открытым.

В соответствии с пунктом первым Положения, утвержденного Постановлением Правительства РФ № 687, неавтоматизированной обработкой являются любые действия с персональными данными, при условии, что использование, уточнение, распространение и уничтожение персональных данных осуществляются при непосредственном участии человека. Причем обработку нельзя признать автоматизированной только потому, что персональные данные содержатся в информационной системе или извлечены из нее.

Когда обработка персональных данных отделом кадров ограничивается лишь фамилией, именем и отчеством – достаточно разработать единый комплексный документ, определяющий политику компании в области обработки персональных данных, как работников, так и иных лиц, вступающих в отношения с компанией и чьи персональные данные обрабатываются.

Если круг субъектов и перечень персональных данных шире (например, компания занимается обработкой и хранением персональных данных своих клиентов), то ограничиться локальными нормативными актами не получится. В таком случае Закон № 152-ФЗ обязывает компанию:

1) уведомить Роскомнадзор о намерении обрабатывать персональные данные;
2) подготовить перечень документов, определяющий порядок обработки и защиты персональных данных. Перечень таких документов достаточно обширный.

Практика показывает, что это:

✓ Приказ о назначении ответственного за организацию обработки персональных данных;

✓ Документ, определяющий политику оператора в отношении обработки персональных данных;

✓ Согласия сотрудников на обработку персональных данных (в т.ч. на передачу третьим лицам и получение у третьих лиц);

✓ Документ, содержащий положения о принятии оператором правовых, организационных и технических мер для защиты персональных данных;

✓ Документы по организации приема и обработке обращений и запросов субъектов персональных данных;

✓ Документы, определяющие категории обрабатываемых персональных данных, особенности и правила их обработки без использования средств автоматизации;

✓ Документ, устанавливающий требования к ведению журналов (реестров, книг), содержащих персональные данные, необходимые для однократного пропуска субъекта персональных данных на территорию;

✓ Документ, устанавливающий требования к хранению материальных носителей содержащих персональные данные;

✓ Документ о классификации информационных систем;

✓ Список лиц, которым необходим доступ к персональным данным, обрабатываемым в информационной системе, утвержденный оператором или уполномоченным лицом;

✓ Документ, устанавливающий порядок обработки персональных данных работников.

Если обработку персональных данных по поручению компании выполняет провайдер, (например, аутсорсинговая бухгалтерская компания), то вышеперечисленный перечень документов дополняется:

1) Письменным поручением на обработку персональных данных. Такое поручение может быть внесено в основной договор об оказании услуг и должно включать не только поручение провайдеру осуществлять от имени компании обработку персональных данных, но и цели такой обработки, перечень действий с ними, их состав, а также обязательство провайдера соблюдать конфиденциальность и безопасность персональных данных, а также требования к их защите.
1) Согласиями на передачу персональных данных провайдеру – от каждого сотрудника

Как видим, перечень документов, регламентирующий обработку персональных данных, достаточно обширный. Чтобы не перегружать документооборот огромным количеством локальных нормативных актов (приказов, положений, инструкций и т.д.), а процесс приема на работу в бесконечный процесс ознакомления с локальными документами, рекомендуется утвердить один документ, регламентирующий все аспекты работы с персональными данными в компании.

В процессе трудовой деятельности любой работник может столкнуться с пристальным вниманием со стороны злоумышленников или конкурентов - как своих, так и конкурентов организации, в которой он работает.

Безопасность собственного персонала - это одно из тех направлений, которое должно быть обеспечено организацией в первую очередь.

Безопасность персонала - это состояние защищенности работников - самого важного ресурса предприятия - от внешних и внутренних угроз, нанесения материального, морального или физического вреда в результате случайных или преднамеренных действий.

Управление безопасностью персонала является сложной проблемой, которая представляет собой управление комплексом организационных и технических мероприятий, снижающих угрозы безопасности персонала на предприятиях.

Приведем примерный перечень некоторых потенциальных угроз персоналу:

- прямое переманивание конкурентами ведущих руководителей и специалистов;
- вербовка сотрудников конкурирующими и криминальными структурами, а в отдельных случаях - правоохранительными органами;
- шантаж или прямые угрозы в адрес конкретных сотрудников с целью склонения их к нарушению доверия со стороны работодателя (т.е. к совершению различных должностных нарушений);
- покушения на сотрудников (прежде всего высших руководителей) и членов их семей.

Подобные угрозы могут быть реализованы в любой организации и по отношению к любому сотруднику, к которому по той или иной причине появился интерес со стороны злоумышленников. Осуществление подобных угроз возможно за счет знания злоумышленниками персональной информации, личных специфических данных о работнике.

Работа кадровых служб всегда связана с накоплением, формированием, обработкой и использованием значительных объемов сведений о всех категориях сотрудников. Эти сведения относятся к персональным данным, которые по своей сути отражают личную и семейную тайну работников, их частную жизнь и входят в круг информации, подлежащей защите от несанкционированного доступа. Бесконтрольное распространение персональных данных может нанести значительный ущерб как физическому лицу - субъекту персональных данных, так и организации, в стенах которой произошла утечка конфиденциальной информации.

В организации защиты персональных данных на локальном уровне особое внимание должно быть уделено элементарным требованиям по правильной, грамотной, квалифицированной кадровой работе, профессиональному уровню подготовки и информационно-правовой культуре сотрудников кадровых подразделений. Несоблюдение сотрудниками кадровых подразделений организационных условий, направленных на защиту персональных данных работников, может способствовать образованию каналов утечки конфиденциальной информации.

Специфика защиты персональных данных лиц, осуществляющих свою профессиональную деятельность на основании трудового договора, проявляется в том, что основополагающие требования по обработке персональных данных устанавливаются нормами федерального законодательства, а порядок осуществления отдельных операций с персональными данными работника (сбор, хранение, использование, распространение) может детализироваться в локальных правовых актах. В соответствии с абз. 7 ч. 1 ст. 22 ТК РФ за работодателями закреплено право принимать локальные нормативно-правовые акты, в которых могут быть отражены вопросы защиты конфиденциальной информации.

Одним из таких локальных нормативно-правовых актов является Положение о персональных данных. Положение определяет основные требования к порядку получения, хранения, комбинирования, передачи или любого другого использования персональных данных работника в связи с трудовыми отношениями в организации.

Разработка и использование эффективной системы обеспечения безопасности персональных данных работников является одной из важных частей системы управления безопасностью персонала, системы охраны жизни и здоровья работников. Образцы документов приведены в конце темы.

1.1. Подбор персонала

Подбор персонала для работы в службе делопроизводства ведется с учетом требований, которые разработаны для должностей, связанных с владением и обработкой конфиденциальных сведений и документов.

Основные требования:

анализ личных и моральных качеств кандидатов на должность,

подписание обязательства о неразглашении защищаемых сведений,

оформление приказом первого руководителя предприятия допуска к конфиденциальной информации,

обучение правилам защиты конфиденциальной информации и регулярное инструктирование по отдельным вопросам защиты,

контроль соблюдения действующих инструкций по работе с конфиденциальными документами и др.

Порядок функционирования отдела кадров должен быть подчинен решению задач обеспечения безопасности персональных сведений, их защиты от неожиданных ситуаций, которые может создать злоумышленник, чтобы завладеть этими сведениями и использовать их в противоправных целях.

2. Процесс защиты персональных данных в службе делопроизводства

В соответствии с требованиями главы 14 Трудового кодекса РФ процесс защиты персональных данных в организации должен быть строго регламентирован. Следует учитывать, что именно регламентация организационных форм и технологии документирования, обработки персональных данных и их неукоснительное соблюдение всеми руководителями и сотрудниками лежат в основе обеспечения надежной защиты персональных данных и, следовательно, обеспечения реальных прав и свобод граждан в трудовой сфере.

В целях выявления состава конфиденциальных сведений и определения основных направлений защиты персональных данных в отделе кадров выделим две большие группы документации:

а) документация по организации работы отдела

б) документация, образующаяся в процессе основной деятельности отдела и содержащая персональные данные в единичном или сводном виде.

Первая группа документации содержит организационно-правовую документацию отдела кадров и включает: положение об отделе, должностные инструкции работников отдела, приказы, распоряжения, указания руководства фирмы, регламентирующие структуру отдела и распределение сфер ответственности между его работниками, рабочие инструкции по выполнению основных функций отдела, ведению документации и формированию персональных данных в комплексы (документы, базы данных и т. п.). Сюда относятся также дела с документацией по планированию, учету, анализу и отчетности в части основной деятельности отдела. Учитывая значительное своеобразие в формировании статуса отдела и организации основных процессов, сопровождающих его деятельность в различных фирмах, конфиденциальный характер этой группы документации определяется тем, что злоумышленник может извлечь из анализа этой документации в конкретной фирме следующие полезные для себя сведения:

распределение функций между отделом кадров и планово-финансовым отделом, бухгалтерией, юридическим отделом, военно-учетным столом и другими подразделениями, т. е. сведения о том, где искать требуемую информацию;

распределение функций внутри отдела кадров между структурными единицами отдела (группами, секторами) и между работниками, т. е. сведения о том, у кого искать требуемую информацию;

регламентацию рабочего процесса по оформлению документации, пропусков, удостоверений, т. е. сведения о том, как можно воспользоваться этим в несанкционированном режиме для фальсификации документов, баз данных;

регламентацию места хранения документов, дел, баз данных, т. е. сведения о том, где и как можно украсть или подменить тот или иной документ, получить требуемую информацию;

регламентацию отчетной и справочной работы, т. е. сведения о том, когда и как можно перехватить требуемую информацию по организационным или техническим каналам.

Любые посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов в отделе кадров. Следует также учитывать, что работник отдела кадров не должен быть осведомлен о порядке работы других сотрудников этого отдела.

Вторая группа - документация, образующаяся в процессе основной деятельности отдела кадров и содержащая персональные данные, включает:

комплекты документов, сопровождающие процесс оформления трудовых правоотношений гражданина (при решении вопросов о приеме на работу, переводе, увольнении и т. п.);

комплекты материалов по анкетированию, тестированию, проведению собеседований с кандидатами на должность;

подлинники и копии приказов по личному составу;

личные дела и трудовые книжки сотрудников;

дела, содержащие основания к приказам по личному составу;

дела, содержащие материалы аттестации сотрудников, служебных расследований и т. п.;

справочно-информационный банк данных по персоналу - учетно-справочный аппарат (картотеки, журналы, базы данных и др.);

подлинники и копии отчетных, аналитических и справочных материалов, передаваемых руководству предприятия, руководителям структурных подразделений и служб;

копии отчетов, направляемых в государственные органы статистики, налоговые инспекции, вышестоящие органы управления и другие учреждения.

Главным моментом в защите персональных и иных конфиденциальных данных является четкая регламентация функций работников отдела кадров и в соответствии с этим - регламентация принадлежности работникам документов, дел, карточек, журналов персонального учета и баз данных.

Для реализации этого положения руководитель фирмы должен издать приказ или распоряжение о закреплении за работниками отдела определенных массивов документов, необходимых им для информационного обеспечения функций, указанных в должностных инструкциях этих работников, утвердить схему доступа работников отдела кадров и руководящего состава фирмы, структурных подразделений к документам отдела, ввести личную ответственность перечисленных должностных лиц и работников за сохранность и конфиденциальность персональных данных.

По каждой функции, выполняемой работником отдела кадров, должен быть регламентирован состав документов, дел и баз данных, с которыми этот работник имеет право работать. Не допускается, чтобы работник мог знакомиться с любыми документами и материалами отдела. Целесообразно, в целях разграничения доступа и разбиения знания персональных данных между работниками, закрепить за разными работниками:

а) документирование оформления трудовых правоотношений (приема, перевода, увольнения и др.);

б) ведение личных дел и трудовых книжек;

в) составление и хранение приказов по личному составу и контрактов;

г) ведение справочно-информационного банка данных.

Распределение сфер деятельности может варьироваться в зависимости от объема работы и штатной численности работников отдела, но разграничение обязанностей и массивов документации должно быть обязательно. Это позволит построить работу отдела в соответствии с указанными выше основополагающими принципами и обеспечить сохранность и конфиденциальность персональных данных. В случае необходимости перераспределения обязанностей среди работников отдела (например, при болезни одного из них, увольнении)

должно быть издано соответствующее распоряжение начальника отдела кадров, в котором регламентируются характер изменений, их срок и дополнения в систему доступа к документам, делам и базам данных. Важно, что в этом распоряжении фиксируется изменение степени осведомленности работников в знании ими персональных данных и сферы личной ответственности за сохранность и конфиденциальность документации.

В сферу ответственности работника, осуществляющего ведение личных дел, входит работа с трудовыми книжками сотрудников фирмы. Трудовые книжки всегда хранятся отдельно от личных дел. Особое внимание обращается на учет в бухгалтерии и отделе кадров чистых бланков книжек и бланков листов-вкладышей. Начальник отдела должен строго контролировать, чтобы подчиненные ему работники не оформляли трудовые книжки на неучтенных бланках (купленных и, как правило, поддельных). Под особым контролем должны находиться операции по проставлению в трудовых книжках печатей и штампов. Целесообразно, чтобы эти операции производил только начальник отдела кадров, так как в противном случае может возникнуть опасность несанкционированного использования печатей и штампов.

2.1. Принципы защиты персональных данных работников

При работе с документами, делами и базами данных кадровой службы должны соблюдаться следующие основополагающие принципы защиты персональных данных:

• личная ответственность руководства организации и работников кадровой службы за сохранность и конфиденциальность персональных данных, а также носителей этой информации;

• разделение (дробление) сведений о персональных данных между разными руководителями организации и работниками службы;

• наличие четкой разрешительной (разграничительной) системы доступа руководителей всех уровней и работников отдела к документам, содержащим персональные данные;

• проведение регулярных проверок наличия традиционных и электронных документов, дел и баз данных у работников службы и кадровых документов в подразделениях организации.

Порядок работы с кадровой документацией должен в полном объеме соответствовать требованиям обращения с конфиденциальными документами. Главным моментом в защите персональных данных является четкая регламентация функций работников кадровой службы и в соответствии с этим регламентация принадлежности работникам функциональных комплексов документов, дел, картотек, журналов персонального учета и баз данных. Любые посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов в кадровой службе. Особенно это касается бланков и документов строгой отчетности. Под посторонним лицом мы понимаем не только злоумышленников или их сообщников, но и сотрудников организации, функциональные обязанности которых не связаны с работой службы.

Следует также учитывать, что работник отдела кадров не должен быть осведомлен о порядке работы других сотрудников этого отдела. Однако, каждый работник должен быть письменно проинформирован о предполагаемых фактах использования его персональных данных при документировании функций кадровой службы, ведении отчетной и отчетно-справочной работы службы. Работник имеет право не разрешить использовать свои персональные данные.

Для реализации положения о личной ответственности работников кадровой службы за доверенные им персональные данные и документы первым руководителем организации должен быть издан приказ о закреплении за каждым работником этой службы определенных массивов документов, необходимых ему для информационного обеспечения функций, указанных в должностных инструкциях, утверждена схема доступа работников службы и руководящего состава организации, структурных подразделений к кадровым документам, установлены формы

ответственности перечисленных должностных лиц и работников за сохранность и конфиденциальность персональных данных. Не допускается, чтобы работник кадровой службы мог знакомиться с любыми документами и материалами службы.

Видимо, целесообразно, чтобы отдельные работники закреплялись за должностными группами персонала организации и выполняли весь объем функций от подбора персонала до хранения документации. В случае необходимости перераспределения обязанностей среди работников службы (например, при болезни одного из них, увольнении) должно быть издано соответствующее распоряжение руководителя службы, в котором регламентируются характер изменений, их срок и дополнения в систему доступа к документам, делам и базам данных.

2.2. Особенности технологии защиты персональных данных

При работе с кадровой документацией следует, прежде всего, соблюдать следующие специфические особенности ее обработки и хранения. Приказы (распоряжения) по личному составу должны составляться, оформляться и храниться в отделе кадров, а не в службе документационного обеспечения управления (делопроизводственной службе). Эту работу следует возложить на отдельного сотрудника кадровой службы или нескольких сотрудников, например, в крупных организациях каждый сотрудник может заниматься приказами по категориям персонала - руководителям, специалистам, рабочим и т.д. Регистрация этих приказов также должна быть передана в кадровую службу.

Материалы, связанные с анкетированием, тестированием, проведением собеседований с кандидатами на должность, помещаются не в личное дело принятого сотрудника, а в специальное дело, имеющее гриф «Строго конфиденциально». Объясняется это тем, что подобные материалы раскрывают личные и моральные качества сотрудника и могут при разглашении, содержащихся в них сведений стать полезными злоумышленнику. Материалы с результатами тестирования работающих сотрудников, материалы их аттестаций формируются в другое дело, также имеющее гриф строгой конфиденциальности.

Особое внимание обращается на сохранность документов личных дел работников. Операции по оформлению, формированию, ведению, закрытию и хранению личных дел выполняются одним работником кадровой службы, который несет личную ответственность за сохранность документов в делах и регламентированный доступ к делам других работников. В случае правомочного изъятия из личного дела документа в описи дела производится запись с указанием основания для подобного действия и нового местонахождения документа. С документа, подлежащего изъятию, снимается копия, которая подшивается на место изъятого документа. Отметка в описи и копия заверяются росписью руководителя и работника кадровой службы. Замена документов в личном деле кем бы то ни было запрещается. Новые, исправленные документы помещаются вместе с ранее включенными в дело.

Приказом первого руководителя должен быть установлен порядок ознакомления или выдачи руководящему составу организации личных дел подчиненных работников. Как правило, знакомиться с личными делами могут: первый руководитель - со всеми личными делами, его заместители - с личными делами курируемых ими подразделений, руководители структурных подразделений - с личными делами сотрудников подразделения. Выдача личных дел на рабочие места руководителей, как правило, не допускается. Личные дела могут выдаваться на рабочие места только первого руководителя предприятия, его заместителя по кадрам и начальника отдела (управления) кадров и в исключительных случаях по письменному разрешению первого руководителя конкретному руководителю структурного подразделения. Дела выдаются (в том числе руководителю кадровой службы или при наличии его письменного разрешения - работнику службы) под роспись в контрольной карточке. В конце рабочего дня личное дело должно быть

возвращено соответствующему сотруднику кадровой службы. При возврате дела тщательно проверяется сохранность документов, отсутствие повреждений документов и включения в дело других документов или подмены документов. Просмотр дела производится в присутствии руководителя. Передача личных дел руководителям через их секретарей или референтов не допускается. Руководители структурных подразделений организации с разрешения руководителя кадровой службы могут знакомиться с личными делами (или при отсутствии личных дел - карточками формы № Т-2) только непосредственно подчиненных им сотрудников; к справочно-информационному банку данных и другой документации кадровой службы они не допускаются. Ознакомление с делами осуществляется в помещении службы под наблюдением работника, ответственного за сохранность и ведение личных дел. Факт ознакомления фиксируется в контрольной карточке личного дела.

Работник организации имеет право знакомиться только со своим личным делом, трудовой книжкой, учетными карточками, отражающими его персональные данные. Он имеет право потребовать внесения изменений и дополнений в свои анкетно-биографические и другие данные, подтвержденных документами. Факт ознакомления работника с личным делом также фиксируется в контрольной карточке.

Ведение и обеспечение сохранности трудовых книжек. В сферу ответственности работника, осуществляющего ведение личных дел, входит работа с трудовыми книжками работников организации. Трудовые книжки всегда хранятся отдельно от личных дел. Особое внимание обращается на учет в бухгалтерии и кадровой службе чистых бланков книжек и бланков листов-вкладышей. Руководитель кадровой службы должен строго контролировать, чтобы трудовая книжка не оформлялась по просьбе работника на неучтенном бланке (купленном и, как правило, фальсифицированном), чтобы от граждан не принимались трудовые книжки, оформленные на подобных бланках или имеющие записи, сделанные с нарушениями соответствующей инструкции. Факт ознакомления работника с записями, произведенными в трудовой книжке, подтверждается его росписью в личной карточке Т-2, в которой эти записи дублируются. Роспись ставится против каждой записи. Кадровая служба должна ежемесячно отчитываться перед бухгалтерией организации о расходовании бланков трудовых книжек и вкладышей. Испорченные бланки трудовых книжек и вкладышей списываются по акту и уничтожаются путем сожжения. На акт наклеиваются вырезанные из бланков номера и серии. Не полученные гражданами при увольнении трудовые книжки хранятся в отделе кадров отдельно от остальных книжек в течение 2 лет, после чего сдаются в архив на 50-летнее хранение.

Под особым контролем должны находиться операции по проставлению в трудовых книжках, на справках и других документах печатей и штампов. Целесообразно, чтобы эти операции производились только руководителем кадровой службы, так как в противном случае может возникнуть опасность несанкционированного использования печатей и штампов. Одновременно руководитель службы контролирует правильность оформления документов. Чистые бланки справок подлежат обязательному учету. Они хранятся у руководителя кадровой службы и выдаются в дневной норме работнику, выдающему справки. По окончании приемных часов этот работник отчитывается перед руководителем службы об израсходованных бланках справок и сдает ему оставшиеся чистыми и испорченные бланки. Проставлять печати и штампы, а иногда и росписи на чистых бланках документов категорически запрещается.

Не менее пристального внимания требует работа со справочно-информационным банком данных по персоналу организации (картотеками, журналами и книгами персонального учета работников). За сохранность и конфиденциальность этого банка данных также должен отвечать специально назначенный сотрудник кадровой службы. Учетная, отчетная и справочная работа кадровой службы наиболее часто формирует каналы несанкционированного получения и незаконного использования персональных данных. В связи с этим первым руководителем организации устанавливается: кто, когда, какие сведения и с какой целью может запрашивать в

отделе кадров. И что особенно важно, определяется порядок дальнейшего хранения сведений, работа с которыми закончена: где эти сведения будут находиться, кто несет ответственность за их сохранность и конфиденциальность. Передаваемые из кадровой службы руководителям отчетные и справочные сведения обязательно документируются в виде сводок, списков, справок и т.п. Устное сообщение сведений, как правило, использоваться не должно, за исключением случаев, когда запрашивается единичная информация, например: дата рождения работника, наличие правительственных наград и т.п. На документах, выходящих за пределы отдела кадров, может ставиться гриф «Конфиденциально» или «Для служебного пользования». В отделе кадров обязательно остаются копии всех плановых, аналитических, отчетных, справочных и иных документов. Целесообразно, чтобы подлинники этих документов после минования в них надобности возвращались в кадровую службу для включения в дело вместо хранящихся там копий.

В структурных подразделениях организации могут быть следующие документы, содержащие персональные данные:

• журнал табельного учета рабочего времени с указанием должностей, фамилий и инициалов работников (находится у сотрудника, ведущего табельный учет - табельщика);

• штатное расписание (штатный формуляр) подразделения, в котором может дополнительно указываться, кто из сотрудников занимает ту или иную должность;

• вакантные должности (находится у руководителя подразделения);

• дело с выписками из приказов по личному составу или копии приказов (распоряжений), касающихся персонала подразделения (находится у табельщика).

Руководитель подразделения может иметь список сотрудников с указанием основных биографических данных каждого из них (год рождении, образование, местожительство, домашний телефон, имя, отчество супруга и др.). Все перечисленные документы следует хранить в соответствующих делах, включенных в номенклатуру дел и имеющих гриф ограничения доступа. Нельзя эти документы хранить в россыпи или записывать указанные сведения на календарях, в личных записных книжках. Не реже одного раза в год работники кадровой службы обязаны проверять наличие этих дел в подразделениях, их комплектность, правильность ведения и уничтожения.

При автоматизированной обработке кадровой информации не рекомендуется данную систему (связанные автоматизированные рабочие места кадровой службы) включать в локальную сеть организации. Внутри кадровой службы локальная сеть (или единичные компьютеры) должна быть снабжена необходимыми средствами программно-аппаратной и криптографической защиты информации, регламентирована жесткой системой разграничения доступа сотрудников службы к обрабатываемой и хранимой информации. В локальную сеть кадровой службы может быть включена рабочая станция (автоматизированное рабочее место) первого руководителя организации.

2.3. Особенности хранения документации

Любые дела, папки с документами, картотеки, машиночитаемые документы, учетные журналы и книги учета хранятся в рабочее и нерабочее время в металлических постоянно запертых шкафах. У каждого работника должен быть свой шкаф для хранения закрепленных за ним массивов документов. Трудовые книжки хранятся в сейфе руководителя кадровой службы, там же хранятся печати, штампы, бланки документов, ключи от рабочих шкафов работников.

Работникам не разрешается при любом по продолжительности выходе из помещения оставлять какие-либо документы или служебные записи на рабочем столе, работающий компьютер. В конце рабочего дня сотрудник службы помещает все рабочие массивы документов в металлический шкаф, запирает его и опечатывает личной печатью. Ключи от шкафов сдаются работниками руководителю кадровой службы под роспись в соответствующем журнале. Категорически запрещается оставлять на рабочем столе в нерабочее время картотеки и другие материалы. Следует также проверить урну для бумаг и убедиться в отсутствии там листов бумаги, которые могут представлять интерес для постороннего лица. Черновики и редакции документов, испорченные бланки, листы со служебными записями в конце рабочего дня уничтожаются в специальной бумагорезальной машине. Уничтожение производится двумя работниками службы. Компьютеры в конце рабочего дня блокируются и отключаются от сети.

2.4. Размещение и организация работы кадровой службы

Кадровая служба организации должна иметь минимально три смежных помещения: комнату для работников службы, кабинет руководителя службы и помещение, в котором размещаются шкафы и сейфы для документов, дел и картотек. Вход в кадровую службу может быть только один. Для ожидающих приема посетителей целесообразно выделить дополнительное помещение за пределами основных помещений службы.

Помещение для размещения шкафов может не иметь окон и оборудуется эффективными техническими средствами пожаротушения. Помещения, шкафы с документацией кадровой службы и компьютеры обеспечиваются охранной сигнализацией. Входная дверь кадровой службы должна быть двойной металлической, окна защищаются решетками. Если кадровая служба использует в работе компьютеры, то помещения службы должны быть оборудованы средствами защиты от технической разведки. По окончании рабочего дня все двери (в том числе внутренние) запираются на надежные замки и опечатываются личной печатью руководителя кадровой службы. Электропитание помещений кадровой службы отключается на центральном щите в помещении охраны организации. Ключи от дверей в опечатанном руководителем службы пенале сдаются работнику охраны под роспись в специальном журнале. Оттиск печати обычно делается на пластилине, в специальной выемке, чтобы печать невозможно было снять и восстановить. Одновременно включается и проверяется надежность средств охранной сигнализации. Сдача под охрану и вскрытие помещений кадровой службы разрешаются только ее руководителю, а в исключительных случаях - заместителю первого руководителя, отвечающему за работу с персоналом.

Перед вскрытием проверяются сохранность и номера печатей, целостность замков и контрольного шнурка (нити). При обнаружении каких-либо попыток проникновения в помещение оно не вскрывается. Составляется акт о выявленной попытке, одновременно об этом факте докладывается лично первому руководителю фирмы и руководителю службы охраны. Дальнейшие действия санкционируются первым руководителем.

Вскрытие рабочих шкафов в отсутствие работника, отвечающего за хранящуюся там документацию, допускается руководителем кадровой службы в присутствии двух работников этой службы. О вскрытии составляется акт с обоснованием причины вскрытия. Акт подписывается указанными лицами. После выполнения необходимых действий шкаф запирается и опечатывается печатью руководителя кадровой службы. При явке на рабочее место сотрудника, отвечающего за хранящуюся в шкафу документацию, им производится проверка наличия документов, дел и других материалов.

Уборка помещения службы осуществляется под наблюдением руководителя кадровой службы. При пожарах, авариях водопроводной и тепловой сети документация кадровой службы

должна быть эвакуирована в безопасное место и обеспечена ее охрана. В условиях возникновения сложных экстремальных ситуаций (стихийных бедствий, военных действий, террористических актов и других подобных событий) и отсутствия возможности эвакуировать чистые бланки трудовых книжек и вкладышей они уничтожаются по акту путем сожжения. В этих условиях трудовые книжки работников могут быть выданы им под роспись в книге учета движения трудовых книжек и вкладышей к ним. Вся остальная кадровая документация должна быть эвакуирована в первую очередь или уничтожена (кроме дел с подлинниками приказов по личному составу и книги учета движения трудовых книжек и вкладышей к ним). Для эвакуации документов в кадровой службе постоянно должна находиться необходимая надежная тара (непромокаемые мешки, контейнеры, чемоданы). За кадровой службой заранее должна быть закреплена грузовая автомашина.

2.5. Регламентирующие документы службы делопроизводства

Организационные и технологические аспекты защиты персональных данных могут найти отражение в двух регламентирующих документах организации.

Во-первых, должно быть разработано положение о персональных данных работников организации, в котором целесообразно четко определить конкретные обязанности руководителей и сотрудников в части использования этих данных в служебных целях. Функциональные обязанности этих лиц следует связать с составом передаваемых им персональных данных. Пользование другими данными им не разрешается. Положение должно содержать схему распределения доступа к персональным данным, состав должностных лиц, дающих разрешение на ознакомление с ними и несущих за это ответственность. Положением должна быть определена форма обязательства указанных лиц за сохранность персональных данных и их конфиденциальность. Одновременно регламентируете порядок ознакомления работников организации со своими персональными данными, документами и учетными формами, в которых эти данные фиксируются, порядок взаимоотношений кадровой службы и работника по поводу сбора, документирования, использования, актуализации, уничтожения и хранения его персональных данных.

Во-вторых, должна быть составлена инструкция, отражающая этапы, процедуры и методы применяемой традиционной или автоматизированной технологии обработки и хранения персональных данных, методы и средства документирования этих данных и формирования баз данных, содержащих эти сведения. В частности, в инструкции следует закрепить технологическую цепочку составления и, оформления приказов и иных кадровых документов, технологические процедуры и операции их хранения, регламентировать порядок формирования, ведения и хранения личных дел работников, ведения и хранения трудовых книжек работников. Следует тщательно определить условия включения документов в личные дела, правила ведения описи документов личного дела, изъятия документов из личного дела, выдачи документов на рабочие места руководителей, проверки сохранности личных дел и документов личного дела. Особое внимание в инструкции следует обратить на организацию и документирование процедур тестирования и анкетирования кандидатов на должность и работников, проведения собеседований и аттестации, порядка ознакомления этих лиц с материалами психологического отбора. В инструкции должна быть определена технология формирования и ведения традиционных или автоматизированных справочно-информационных систем (картотек, журналов, баз данных), обеспечивающих поисковые, учетные и отчетные функции при работе сотрудников кадровой службы с персональными данными работников. Установлено, в какие документы и учетные формы следует ввести необходимые зоны и графы для отражения факта

ознакомления работников со своими персональными данными. В соответствии с разработанным положением и инструкцией должна быть построена практическая работа руководителей организации, сотрудников кадровой и иных служб, использующих в работе персональные данные работников.

2.6. Работа с посетителями в кадровой службе

Говоря о технологии защиты информации в кадровой службе, необходимо учитывать, что помимо операций с документами работники отдела кадров значительную часть времени тратят на прием посетителей. Этот вид работы также должен быть строго регламентирован, так как посетители могут представлять определенную угрозу информационной безопасности кадровой службы и физической безопасности ее работников. Важно, чтобы прием посетителей осуществлялся только в те часы, которые ежедневно выделяются для этой цели. В другое время в помещении кадровой службы не могут находиться посторонние лица, в том числе работники организации. Целесообразно, чтобы приемные часы были разными для работников организации и лиц, не входящих в эту категорию. Подобное разграничение необходимо ввиду того, что в числе последней группы лиц может быть злоумышленник, который будет слышать переговоры работников организации, сможет познакомиться с работниками, получить информацию о их привычках, чертах характера, что в последующем может стать основой для формирования канала несанкционированного доступа к ценной информации. Прием посетителей должен быть организован таким образом, чтобы в помещении службы не было лиц, ожидающих приема. Не должны возникать так называемые «живые очереди». Лица, ожидающие приема, всегда подсознательно или умышленно прослушивают переговоры работника кадровой службы и посетителя. Злоумышленник может эти переговоры записывать с помощью диктофона или миниатюрной видеокамеры. В часы приема посетителей работники службы не должны выполнять функции, не связанные с приемом, вести служебные и личные переговоры по телефону. На столе работника, ведущего прием, не должно быть никаких документов, кроме тех, которые касаются данного посетителя. Ответы на вопросы даются только лично тому лицу, которого они касаются.

При выдаче справки с места работы необходимо удостовериться в личности работника, которому эта справка выдается. Не разрешается выдавать ее родственникам или сослуживцам лица, которому требуется справка. Справка выдается на основании учетной карточки № Т-2, а не пропуска, так как работник при увольнении мог не сдать пропуск или удостоверение. Заполненный бланк справки подписывается руководителем кадровой службы. Передает справку на подпись работник службы, а не посетитель. Одновременно руководитель службы ставит на справке печать. За получение справки работник организации расписывается в журнале учета выдачи справок.

Не допускается отвечать на вопросы, связанные с передачей персональной информации, по телефону или факсу. Ответы на правомерные письменные запросы других учреждений и организаций даются с разрешения первого руководителя организации и только в письменной форме и том объеме, который позволяет не разглашать излишний объем персональных сведений. По возможности персональные данные обезличиваются.

В помещении кадровой службы в часы приема посторонних лиц может находиться работник службы безопасности организации. Целесообразно также наличие сигнализации, оповещающей работников этой службы о необходимости немедленно вмешаться в сложившуюся ситуацию. На столе работника кадровой службы не должно быть тяжелых предметов: подставок под календарь, пепельниц и т.п. В целях удобного доступа посетителей в кадровую службу помещения службы должны располагаться на первом этаже, поблизости от входа в здание. В

часы приема лиц, не являющихся работниками организации, вход в отдел должен быть свободным для всех желающих. Проход посторонних лиц в помещение отдела контролируется сотрудником службы безопасности: посетитель идентифицируется по паспорту или служебному удостоверению, при необходимости посетителя провожают. Бесконтрольное нахождение посторонних лиц в здании организации не допускается. Проход посторонних лиц на другие этажи здания и помещения может быть блокирован охраной организации.

3. Ответственность за нарушение закона 152-ФЗ

Нарушить требования к работе с персональными данными и заработать штраф от Роскомнадзора можно совершенно случайно. Самые распространенные нарушения:

1. Документы оставлены на столе

Очень часто в штатной бухгалтерии и маленьких бухгалтерских фирмах стопки бумаг свалены на рабочем столе, и никто не отслеживает, есть ли в этих бумагах личные данные. Однако оставлять личные документы сотрудников в общедоступном месте нельзя, так как личная информация может оказаться в руках посторонних (коллег, представителей компаний-поставщиков).

Штраф: для руководителя компании – до 10 000 руб.; для компании – до 50 000 руб.; для ИП – до 20 000 руб. (ч. 6 ст. 13.11 КоАП РФ).

Пример защиты персональных данных. Необходимо разработать порядок работы с персональной информацией. В нем четко прописать запрет оставлять на столе бумаги с личными данными и выносить их за пределы кабинета. Документы должны храниться в сейфе или шкафу, где доступ к ним будет ограничен.

2. Работнику не выдали документы с его персональными данными

Речь идет о невыдаче расчетных листков работникам, сведений о стаже и других бумаг. Это также является сокрытием от сотрудника его персональных данных.

Штраф: для руководителя компании – до 5 000 руб.; для компании – до 50 000 руб.; для ИП – до 5 000 руб. (ст. 5.27 КоАП РФ).

Пример защиты персональных данных. Высылать работникам расчетные листки на электронную почту либо сообщением на корпоративном сайте вашей организации. Сведения о стаже надо выдать в течение 3-х календарных дней с момента, когда работник за ними обратился, а также в день увольнения.

3. Забыли обновить данные работника

Данные обновляются по просьбе сотрудника, например, в случае смены фамилии после замужества или адреса регистрации. Если компания этого не сделает, то нарушит правила работы с персональными данными.

Штраф: для руководителя компании – до 10 000 руб.; для компании – до 45 000 руб.; для ИП – до 20 000 руб. (ч. 5 ст. 13.11 КоАП РФ).

Пример защиты персональных данных. Если сотрудник принес документы, подтверждающие изменения, немедленно вносите новые данные в базу.

4. Размещение личной информации в общедоступном месте

Случается, что личные данные по чистой случайности попадают на стенд или корпоративный сайт – например, в качестве образца заявления на имущественный вычет главбух разместил на стенде копию заявления, полученного от сотрудника компании. Если в документе указаны личные реквизиты, то это нарушение, поскольку сотрудник не давал согласие на обнародование его реквизитов.

Штраф: для руководителя компании – до 20 000 руб.; для компании – до 75 000 руб. (ч. 2 ст. 13.11 КоАП РФ).

Пример защиты персональных данных. Никогда не использовать реальные документы в качестве образцов, а подготовить образцы с использованием вымышленных сведений.

5. Сообщение имени, адреса и телефона сотрудника третьим лицам

Информацию о сотрудниках может запросить банк или коллекторское агентство. Без согласия сотрудника такая передача сведений является нарушением.

Штраф: для руководителя компании – до 10 000 руб.; для компании – до 50 000 руб. (ч. 1 ст. 13.11 КоАП РФ).

Пример защиты персональных данных. Передавать информацию о сотруднике по просьбе другой организации или физлицам только в том случае, если работник выдал им доверенность на получение сведений.

Возможные нарушения в области защиты персональных данных и суммы штрафов мы привели в таблице:

За что могут штрафовать	**Сумма штрафа**
Персональные данные обрабатываются не в тех целях, на которое дано согласие Например, персональные данные работника обрабатываются в целях расчета заработной платы, ведения кадрового делопроизводства, но никак не для оформления кредита, открытия лицевых счетов в банках, продажи чего-либо. В согласии на обработку персональных данных обязательно указываются цели обработки – это требование Закона 152-ФЗ.	от 30 000 до 50 000 руб.
Обработка персональных данных отделом кадров без письменного согласия (когда оно, естественно, требуется)	от 15 000 до 75 000 руб.
Политика по обработке персональных данных не опубликована или отсутствует в свободном доступе (на стенде, на сайте и т.д.)	от 15 000 до 30 000 руб.
Оператор персональных данных не отреагировал на запрос сотрудника (субъекта персональных данных) Например, на электронную почту приходит регулярная рассылка с сайта ***, принадлежащего компании ААА. Получатель рассылки направляет в компанию ААА запрос о подтверждении факта обработки его персональных данных, их состава, целей такой обработки и т.д. В течение 30 дней компания ААА должна дать официальный ответ. Если такого ответа не последовало, то это нарушение.	от 20 000 до 45 000 руб.

Нарушены условия защиты бумажных документов, содержащих персональные данные Например, произошла утечка данных вследствие случайного доступа постороннего лица, уничтожение персональных данных, их распространение и т.д.	от 25 000 до 50 000 руб.

4. Примерный образец Положения о защите персональных данных

ООО "Общество"

ПОЛОЖЕНИЕ

_____ N _____

О защите персональных данных

Утверждаю

Руководитель организации

_____ И.О. Фамилия

дата

1. Общие положения

1.1. Положение о защите персональных данных (далее - Положение) определяет порядок сбора, хранения, комбинирования, передачи и любого другого использования персональных данных в соответствии с законодательством Российской Федерации.

1.2. Положение разработано в соответствии с Конституцией Российской Федерации, Гражданским кодексом Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации", Федеральным законом от 27.07.2006 N 152-ФЗ "О персональных данных", иными нормативными актами, действующими на территории Российской Федерации.

3. Понятие и состав персональных данных

Персональные данные - информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника, а также любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

2.2. К персональным данным относятся:

- сведения, содержащиеся в документах, удостоверяющих личность;
- информация, содержащаяся в трудовой книжке;
- информация, содержащаяся в страховом свидетельстве государственного пенсионного страхования;
- сведения, содержащиеся в документах воинского учета;
- сведения об образовании, квалификации или наличии специальных знаний или подготовки;
- информация о состоянии здоровья в случаях, предусмотренных законодательством;
- сведения, содержащиеся в свидетельстве о постановке на учет физического лица в налоговом органе на территории Российской Федерации;
- сведения о семейном положении;

- информация о заработной плате;
- другая персональная информация.

2.3. К документам, содержащим информацию персонального характера, относятся:

- документы, удостоверяющие личность или содержащие информацию персонального характера;
- учетные документы по личному составу, а также вспомогательные регистрационно-учетные формы, содержащие сведения персонального характера;
- трудовые договоры с работниками, изменения к трудовым договорам, договоры о материальной ответственности с работниками;
- распорядительные документы по личному составу (подлинники и копии);
- документы по оценке деловых и профессиональных качеств работников при приеме на работу;
- документы, отражающие деятельность конкурсных и аттестационных комиссий;
- документы о результатах служебных расследований;
- подлинники и копии отчетных, аналитических и справочных материалов, передаваемых руководству предприятия, руководителям структурных подразделений и служб;
- копии отчетов, направляемых в государственные органы статистики, налоговые инспекции, вышестоящие органы управления и другие учреждения;
- документы бухгалтерского учета, содержащие информацию о расчетах с персоналом;
- медицинские документы, справки;
- др. документы, содержащие сведения персонального характера.

3. Получение персональных данных

3.1. Персональные данные работника предоставляются самим работником. Если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Работодатель должен сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение.

3.2. Работник обязан предоставлять работодателю достоверную персональную информацию. При изменении персональных данных работник должен письменно уведомить об этом работодателя в срок, не превышающий 14 дней. Работодатель имеет право запрашивать у работника дополнительные сведения и документы, подтверждающие их достоверность.

3.3 Работодатель не имеет права получать и обрабатывать персональные данные работника о его политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со ст. 24 Конституции Российской Федерации работодатель вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия.

3.4. Работодатель не имеет права получать и обрабатывать персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных ТК РФ или иными федеральными законами.

3.5. При принятии решений, затрагивающих интересы работника, работодатель не имеет права основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного получения.

4. Обработка и передача персональных данных

4.1. Обработка персональных данных работника осуществляется исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

4.2. Допуск к персональным данным работника разрешен должностным лицам, которым персональные данные необходимы для выполнения конкретных трудовых функций. Список лиц, имеющих право доступа к персональным данным работников, представлен в Приложении N 1 к настоящему Положению.

4.3. Внешний допуск к персональным данным работников имеют сотрудники контрольно-ревизионных органов при наличии документов, являющихся обоснованием к работе с персональными данными.

4.4. При обработке персональных данных, не связанных с исполнением трудового договора, работодатель обязан получить согласие работника на обработку его персональных данных в письменном виде. Форма согласия на обработку персональных данных работника представлена в Приложении N 2.

4.5. Требования к передаче персональных данных:

- не сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в других случаях, предусмотренных законодательством РФ;

- не сообщать персональные данные работника в коммерческих целях без его письменного согласия;

- предупредить лиц, получающих персональные данные работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено;

- осуществлять передачу персональных данных работника в пределах одной организации, у одного индивидуального предпринимателя в соответствии с локальным нормативным актом, с которым работник должен быть ознакомлен под роспись;

- разрешать доступ к персональным данным работников только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций;

- не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции;

- передавать персональные данные работника представителям работников в порядке, установленном законодательством РФ, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.

4.6. Подразделения, а также сотрудники организации, в ведение которых входит работа с персональными данными, обеспечивают защиту персональных данных от несанкционированного доступа и копирования.

4.7. Защита персональных данных работников от их неправомерного использования или утраты обеспечивается работодателем за счет его средств в порядке, установленном законодательством РФ.

5. Хранение персональных данных

5.1. Служба кадров и иные подразделения (бухгалтерия, служба безопасности, служба системного администрирования и т.д.) организуют хранение и использование персональных данных работников в соответствии с законодательством РФ, настоящим Положением и другими локальными нормативными актами организации, регламентирующими порядок работы с персональными данными работников.

5.2. Хранение персональных данных работников осуществляется на электронных носителях, а также в бумажном варианте.

5.3. Доступ к программному обеспечению, а также к персональной информации, хранящейся на электронных носителях, строго регламентирован (Приложение N 1) и осуществляется при введении личного идентификатора и пароля пользователя.

5.4. Документы персонального характера хранятся в сейфах подразделений, ответственных за ведение и хранение таких документов.

5.5. Помещения, в которых хранятся персональные данные работников, оборудуются надежными замками и системой сигнализации.

6. Уничтожение персональных данных

6.1. Документы, содержащие персональные данные, подлежат хранению и уничтожению в порядке, предусмотренном архивным законодательством Российской Федерации.

6.2. Персональные данные работников подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в достижении таких целей.

7. Права работника по обеспечению защиты своих персональных данных

7.1. Работники имеют право на:

- полную информацию о своих персональных данных и обработке этих данных;
- свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные работника, за исключением случаев, предусмотренных федеральным законом;
- определение своих представителей для защиты своих персональных данных;
- доступ к своим медицинским данным с помощью медицинского специалиста по своему выбору;

- требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением законодательства РФ;
- требование об извещении работодателем всех лиц, которым ранее были сообщены неверные или неполные персональные данные работника, обо всех произведенных в них исключениях, исправлениях или дополнениях;
- обжалование в суд любых неправомерных действий или бездействия работодателя при обработке и защите его персональных данных.

8. Обязанности и ответственность работодателя за нарушение норм, регулирующих обработку и защиту персональных данных

8.1. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, несут ответственность в соответствии с законодательством РФ:

- дисциплинарную;
- материальную;
- гражданско-правовую;
- административную;
- уголовную.

8.2. Представление работником подложных документов является основанием для вынесения дисциплинарных взысканий вплоть до увольнения.

9. Заключительные положения

9.1. Положение обязательно для всех работников общества.

9.2. Работники и их представители должны быть ознакомлены под расписку с документами организации, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области. Форма расписки представлена в Приложении N 3 к настоящему Положению.

СОГЛАСОВАНО

Главный бухгалтер

Начальник службы кадров

Примерный образец

Приложение N 1

к Положению о защите персональных данных

СПИСОК ЛИЦ,

ИМЕЮЩИХ ПРАВО ДОСТУПА К ПЕРСОНАЛЬНЫМ ДАННЫМ РАБОТНИКОВ

N п/п	Должность	Ф.И.О.	Перечень персональных данных, к которым допущен сотрудник	Примечание

Примерный образец

Приложение N 2

к Положению о защите персональных данных

СОГЛАСИЕ РАБОТНИКА на обработку его персональных данных

Я, _____,

(Ф.И.О. полностью, должность)

являясь работником _____ (далее - Оператор), находящегося по адресу: _____, своей волей и в своем интересе выражаю согласие на обработку моих персональных данных Оператором для формирования общедоступных источников персональных данных (справочников, адресных книг, информации в СМИ и на сайте организации и т.д.), включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), распространение (в том числе передачу) и уничтожение моих персональных данных, входящих в следующий перечень общедоступных сведений:

1. Фамилия, имя, отчество.
2. Рабочий номер телефона и адрес электронной почты.
3. Сведения о профессии, должности, образовании.
4. Иные сведения, предоставленные мной для размещения в общедоступных источниках персональных данных.

Также выражаю согласие на получение и передачу моих персональных данных органам местного самоуправления, государственным органам и организациям для целей обеспечения соблюдения законов и иных нормативных правовых актов, содействия в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности, контроля количества и качества выполняемой работы и обеспечения сохранности имущества, оформления доверенностей, прохождения конкурсного отбора, прохождения безналичных платежей на мой банковский счет. Для этих целей дополнительно могут быть получены или переданы сведения о дате рождения, гражданстве, доходах, паспортных данных, предыдущих местах работы, идентификационном номере налогоплательщика, свидетельстве государственного пенсионного страхования, допуске к сведениям, составляющим государственную тайну, социальных льготах и выплатах, на которые я имею право в соответствии с действующим законодательством.

Вышеприведенное согласие на обработку моих персональных данных представлено с учетом п. 2 ст. 6 и п. 2 ст. 9 Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных" (ред. от 23.12.2010), в соответствии с которыми обработка персональных данных, осуществляемая на основе федерального закона либо для исполнения договора, стороной в котором я являюсь, может осуществляться Оператором без моего дополнительного согласия.

Настоящее согласие вступает в силу с момента его подписания на срок действия трудового договора с Оператором и может быть отозвано путем подачи Оператору письменного заявления.

"__" _____ 20__ г.

_____

(подпись и фамилия, имя, отчество прописью полностью)

Примерный образец

Приложение N3

к Положению о защите персональных данных

РАСПИСКА

Я, _____,

(фамилия, имя, отчество работника)

_____,

(структурное подразделение, должность)

ознакомлен с Положением о защите персональных данных, права и обязанности в области защиты персональных данных мне разъяснены.

"__" _____ 20__ г. _____ И.О. Фамилия

(подпись)