

Федеральное государственное автономное
образовательное учреждение
высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Юридический институт
Кафедра трудового и экологического права

УТВЕРЖДАЮ

Заведующий кафедрой

_____ Е.И. Петрова

подпись

« ____ » _____ 2017 г.

БАКАЛАВРСКАЯ РАБОТА

40.03.01 - Юриспруденция

код – наименование направления

Защита персональных данных работника в России

тема

Руководитель

подпись, дата

к.ю.н., доцент

должность, ученая степень

С.П. Басалаева

инициалы, фамилия

Выпускник

подпись, дата

Т.Д. Ложникова

инициалы, фамилия

Красноярск 2017

СОДЕРЖАНИЕ

Введение.....	3
1 Теоретико-правовые основы института персональных данных в трудовых правоотношениях	6
1.1 Международно-правовые основы защиты персональных данных...	6
1.2 Понятие персональных данных в трудовом праве.....	12
1.3 Виды персональных данных.....	14
2 Правовое содержание защиты персональных данных работника.....	20
2.1 Обработка персональных данных работников.....	20
2.2 Хранение, использование и передача персональных данных работников	30
2.3 Права работника как субъекта персональных данных	36
2.4 Ответственность за нарушение порядка работы с персональными данными.....	39
3 Локальное нормативно-правовое регулирование защиты персональных данных в трудовых правоотношениях.....	52
Заключение.....	58
Список использованных источников.....	62
Приложения А-Б.....	69

ВВЕДЕНИЕ

Современный этап развития общества характеризуется возрастающей ролью информационной сферы, представляющей собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации. В настоящее время технические средства позволяют производить сбор и обработку существенных объемов социально значимых сведений, необходимых для эффективного функционирования государственных механизмов, протекания общественных процессов, а также реализации прав человека. Стремительное развитие информационных технологий дает возможность получать доступ и использовать различные банки данных практически любым субъектам информационных отношений. Постоянно ускоряющаяся информатизация общества и активное развитие открытых информационных систем значительно упрощают утечку и иные формы незаконного доступа к личной информации, что делает задачу обеспечения необходимой правовой защиты персональной информации особо актуальной и значимой.

Появление в российском трудовом праве норм о защите персональных данных работника продиктовано необходимостью реализации в сфере труда общепризнанных норм и принципов международного права, применение которых гарантировано Конституцией Российской Федерации [1], которая в ст. 23 и 24 устанавливает, что каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну; сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускается. Жизнедеятельность человека предполагает предоставление информации о себе другим членам общества, а общественные отношения по предоставлению и охране информации регулируются нормами права. Так, эффективное управление поведением работника в процессе труда возможно лишь при наличии достоверных сведений о его личности, представленных в достаточном объеме. В Трудовом кодексе Российской Федерации (ТК РФ) [4]

в специальной главе работодателю разрешено получать, хранить, комбинировать, использовать персональные данные нанятого им работника; законодатель установил общие требования к обработке персональных данных работника и определил гарантии их защиты.

Персональные данные окружают нас повсюду, однако правильно работать с ними умеют далеко не все работодатели. Российское законодательство о защите персональных данных является относительно новым, и существует множество нерешенных вопросов, что зачастую препятствует выполнению работодателем необходимых требований действующего законодательства о персональных данных.

В процессе работы с персональными данными возникает множество вопросов, связанных с применением Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» [7], которым регулируются отношения, связанные с обработкой персональных данных, осуществляемой государственными органами, органами местного самоуправления, муниципальными органами, юридическими лицами, физическими лицами. Зачастую работодатель пренебрегает мерами сохранности персональных данных своих работников, что чревато их несанкционированным распространением.

Учитывая вводимые изменения Федеральным законом от 07.02.2017г. №13-ФЗ в области персональных данных по ужесточению административной ответственности с 01.07.2017г. [8] , проблема защиты персональных данных работников в любой организации является весьма актуальным направлением в наши дни.

В связи с этим изучение данной проблемы приобретает особую значимость как с точки зрения углубления и совершенствования теоретических и прикладных основ, так и с позиции возможности использования результатов в формировании политики в области персональных данных работодателей, позволяющей выполнять необходимые требования действующего законодательства о персональных данных.

Таким образом, в современных социально-экономических условиях в связи с формированием в стране рыночной экономики и обострением социальных проблем роль защиты персональных данных работника значительно возрастает.

Цель работы - разработать рекомендации действий работодателя при формировании политики по защите персональных данных.

Для достижения поставленной цели необходимо решить следующие задачи:

-изучить теоретико-правовые основы института персональных данных в трудовых правоотношениях;

- проанализировать международно-правовые основы защиты персональных данных;

- изучить правовое содержание защиты персональных данных работника;

- проанализировать ответственность за нарушение норм, регулирующих защиту персональных данных работника;

-выявить перечень обязательных документов для работодателя при работе с персональными данными;

- разработать проект положения «О защите персональных данных».

Объектом исследования является общественные отношения, складывающихся в сфере защиты персональных данных в рамках трудовых отношений.

Предметом исследования являются нормы отечественного и зарубежного права, регламентирующие использование и защиту персональных данных работника, нормативно-правовые акты о защите персональных данных работников, принятые на международном уровне, в Российской Федерации, на локальном уровне отдельных организаций, практика их применения.

Работа состоит из введения, трех глав, заключения, списка использованных источников и приложений.

1 Теоретико-правовые основы института персональных данных в трудовых правоотношениях

1.1 Международно-правовые основы защиты персональных данных

В странах Европы и Америки информатизация началась раньше, чем в России, и как следствие – достаточно развит институт защиты персональных данных. Обратимся к зарубежному законодательству, в котором описаны принципы защиты персональных данных при их обработке.

Право на защиту персональных данных является производным от права человека на невмешательство в личную жизнь. Последнее прямо закреплено во Всеобщей декларации прав человека 1948 г. (ст. 12), принятой Генеральной Ассамблеей ООН 10 декабря 1948 г, Пакте ООН о гражданских и политических правах 1966 г. (ст. 17) и Европейская конвенция о защите прав человека и основных свобод, принятая Советом Европы 4 ноября 1950 г. (ст. 8). В указанных актах установлено право на уважение частной и семейной жизни, признаны незаконными какие бы то ни было посягательства на честь и достоинство человека.

Всеобщая декларация прав человека от 10 декабря 1948 г. гласит: «Никто не может подвергаться произвольному вмешательству в его личную и семейную жизнь, произвольным посягательствам на неприкосновенность его жилища, тайну его корреспонденции или на его честь и репутацию. Каждый человек имеет право на защиту закона от такого вмешательства или таких посягательств» [26].

Ключевые принципы неприкосновенности частной жизни и индивидуальных свобод узаконила Директива о защите неприкосновенности частной жизни и международных обменов персональными данными от 23 сентября 1980 г.:

– объем собираемых персональных данных должен иметь пределы;

- персональные данные должны соответствовать целям, в которых они будут использоваться;
- персональные данные не должны разглашаться;
- создание механизмов, позволяющих работнику узнавать о наличии в обращении и о содержании его персональных данных, а также требовать их исправления [17].

Конвенция СЕ «О защите физических лиц при автоматизированной обработке персональных данных» 1981 г. является единственным юридически обязывающим международным договором Российской Федерации. Данная конвенция была ратифицирована нашей страной. Последствием этой ратификации стало принятие Федерального закона «О персональных данных» и ряда других федеральных нормативных правовых актов. Конвенция СЕ определяет основные принципы защиты персональных данных, к числу которых относятся:

- соблюдение требований к качеству данных (собираются и обрабатываются на справедливой и законной основе; собираются и хранятся для законных целей и не используются иным образом; являются адекватными, точными, обновляемыми и относящимися к делу; сохраняются в форме, позволяющей идентифицировать субъекта данных, и не дольше, чем этого требует цель хранения этих данных);

- введение специальной категории данных в целях защиты от дискриминации. К их числу относятся данные о расовой принадлежности, политических взглядах, религиозных и иных убеждениях, а также данные о здоровье и половой жизни. Они не могут подвергаться автоматической обработке, если внутреннее законодательство не установило для них специальные гарантии;

- защита персональных данных посредством принятия надлежащих мер безопасности, направленных на предотвращение их несанкционированного уничтожения, потери, изменения или распространения;

- предоставление субъектам персональных данных дополнительных гарантий (получать в разумный срок доступ к своим данным; знать о базах персональных данных и целях их создания; прибегать к средствам правовой защиты в случае неисполнения предыдущего требования; требовать исправления или уничтожения недостоверных данных) [23].

Обеспечение уважения прав и основных свобод каждого человека и в особенности его права на неприкосновенность личной сферы в связи с автоматической обработкой касающихся его персональных данных - цель Конвенции.

Статья 7 этой Конвенции обязывает лиц, осуществляющих сбор персональных данных, принимать надлежащие меры для охраны персональных данных, накопленных в автоматизированных базах данных, от случайного или несанкционированного разрушения или случайной утраты, а равно от несанкционированного доступа, изменения или распространения.

Согласно Директиве Европейского Союза 95/46/ЕС2 введены следующие критерии обработки персональных данных: обработка возможна при наличии однозначного согласия субъекта, или обработка необходима для исполнения договора, стороной которого является субъект данных или в целях принятия мер по просьбе субъекта данных до заключения договора; или обработка необходима для соблюдения юридического обязательства, субъектом которого является оператор и т.д.

Как отмечают некоторые ученые, в Европейском Союзе сложился комплексный механизм защиты персональных данных:

– наличие общеевропейской нормативной базы, действие национальных законодательных актов, регулирующих вопросы персональных данных;

– правовая четкость основных принципов права по защите персональных данных;

– наличие европейских надзорных и консультативных органов, а также создание национальных административных органов по защите персональных данных;

– нормативная определенность правового статуса – основных прав, свобод и обязательств;

– наличие правовой определенности по условиям передачи персональных данных третьим лицам.

Институт защиты персональных данных сегодня уже не является той категорией, которую можно регулировать только национальным правом. Важнейшей особенностью современных автоматизированных информационных систем являются наднациональность многих из них, выход их за пределы границ государств [37].

Институт защиты персональных данных является наглядным примером развития международного и обогащения российского трудового права. Особенностью регулирования защиты персональных данных работников на международном уровне является рекомендательный характер правовых норм и институтов, воздействующих на эти отношения.

Вопросы защиты информации личного характера подробно регламентированы Кодексом практики МОТ по защите персональных данных работников (далее – Кодекс). Этот документ был подготовлен экспертами МОТ в 1995-1996 годах. Он имеет классическую структуру специализированного акта. В соответствии со своими целями он содержит подробное разъяснение употребляемой терминологии, пределов своего применения, принципов и правил сбора, хранения, передачи и иного использования персональных данных работника. Отдельно рассматриваются вопросы реализации индивидуальных и коллективных прав для достижения целей документа. К Кодексу составлен комментарий для подробного разъяснения отдельных вопросов. Его издание ориентировано в первую очередь на добровольное внедрение правовых механизмов по защите персональных данных в законодательство отдельных стран. При анализе

отечественных и зарубежных актов можно убедиться в их тесной связи с данным документом.

Персональными данными Кодекс называет любую информацию, связанную с отождествлением или способностью к отождествлению конкретного работника (п. 3.1. Кодекса). «Способность к отождествлению» означает, что в данное понятие не входит информация, которая собирается необоснованно длительное время и не требуется для того, чтобы установить личность определенного работника. Обработка персональных данных включает в себя сбор, хранение, передачу, комбинирование и любое иное использование персональных данных (п. 3.2. Кодекса). Данная терминология соответствует принятым международным понятиям в сфере информационного обмена.

Обоснованность их предоставления работодателю трудовыми отношениями с работником является основным принципом работы с персональными данными работника (п.п. 5.1.-5.4. Кодекса). Это правило определяет цели, пределы и формы сбора информации о работнике. Работник не должен быть поставлен в вынужденную ситуацию объяснения того, что затребованная информация касается его личной жизни, и что он не хочет разглашать эти сведения. Это обязанность работодателя - пояснить и доказать работнику, что для их совместной деятельности ему (работодателю) необходимы определенные сведения о личности работника.

Надлежащую сохранность информации обеспечивает работодатель. Обязанность охватывает не только требование хранить информацию надлежащим образом, но и запрет физического доступа к сведениям посторонних лиц. Сроки хранения определяются требованиями законодательства либо желанием работника. Ситуация решается в зависимости от категории сведений. Желание работника и требования законодательства также являются определяющими факторами при передаче информации третьим лицам.

Применительно к защите персональных данных Кодекс выделяет индивидуальные и коллективные права (соответственно 11 и 12 главы Кодекса). Индивидуальные права являются первичными и включают в себя право работника знать о собираемой и собранной о нем информации, получения копий, права доступа, на внесение исправлений в записи, быть оповещенным в случае изменения сведений.

Кодекс содержит прямые отсылочные нормы к иным документам и законодательству по смежным вопросам. Это прежде всего законодательство о защите личной жизни граждан, об информационном обороте. Особенностью этой законодательной сферы является то, что вопросы получения, хранения, передачи и иного использования информации регулируются комплексно. Отдельные акты касаются защиты работника от дискриминации, регулирования правовых и этических вопросов во время наблюдения за работником на рабочем месте, использования медицинской информации о его здоровье, использования электронных средств обработки данных, информационному взаимодействию со службами занятости. В настоящее время Кодекс является самым подробным документом о защите персональных данных на международном уровне [38].

Результаты анализа международно-правовых документов в области защиты персональных данных позволяют определить приоритет международных норм в развитии института персональных данных, выделить единые принципы для всех демократических государств вне зависимости от особенностей их правовых систем, раскрыть содержание права лица на осуществление контроля за обработкой касающихся его персональных данных и критерии его ограничения, выделить условия деятельности независимых надзорных органов по защите прав и основных свобод человека в связи с обработкой его персональных данных.

Результаты обобщения зарубежного опыта в области защиты персональных данных позволяют сделать вывод, что создание гармоничной системы защиты персональных данных невозможно без установления

баланса между интересами индивида, общества и государства, который должен базироваться:

- на развитии информатизации и обработки персональной информации государственными и частными структурами в целях повышения эффективности их функционирования, но в рамках необходимой достаточности для рационального принятия решений в экономической, социальной и управленческой сферах;

- на соблюдении неприкосновенности частной жизни в такой степени, чтобы обеспечить автономию и свободу личности от неоправданного вмешательства со стороны других людей, государственных органов власти или каких-либо общественных организаций;

- на установлении независимых форм контроля в области защиты прав и основных свобод человека в связи с обработкой его персональных данных.

1.2. Понятие персональных данных в трудовом праве

Основополагающие акты правового регулирования сферы персональных данных – глава 14 «Защита персональных данных работника» Трудового кодекса РФ и Федеральный закон «О персональных данных». Также приняты одновременно Федеральные законы от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации» и N 152-ФЗ «О персональных данных». Из Федерального закона «О персональных данных» следует, что его основной целью является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну (ст. 2).

В Законе «О персональных данных» (ст. 3) дано следующее определение: персональные данные - это любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных) [7].

Итак, персональными данными является любая информация, с помощью которой лицо можно идентифицировать (определить). Далее в определении уточняется, что к информации о лице относятся фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, имущественное и социальное положение, профессия, образование, доходы и другая информация.

В качестве «другой» информации может выступать биометрическая информация о лице; данные о супруге, детях, других членах семьи; индивидуальные средства коммуникации (адрес электронной почты, номер телефона); сведения о событиях и обстоятельствах жизни лица, позволяющие его идентифицировать, в том числе аудио - и видеофайлы, и т.д. Перечень сведений, которые могут быть отнесены к персональным данным, является открытым [49].

В соответствии со ст. 85 Трудового кодекса РФ [4] персональные данные работника – информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся определенного работника. Это сведения, которые могут охарактеризовать человека именно как работника. Каких-либо иных критериев, как и конкретного перечня, персональных данных работника, Трудовой кодекс РФ не устанавливает. Как правило, это информация, необходимая для заключения трудового договора, назначения на другую должность, заполнения личной карточки Т-2 и т.д.

Работник предоставляет свои персональные данные работодателю лишь в том предусмотренном законами объеме и необходимом для заключения трудового договора и оформления работника на работу (статья 65 Трудового кодекса РФ). Работодатель не вправе требовать от работника предоставления каких-либо сведений, которые касаются его частной жизни. В случае возникновения у работодателя необходимости получения такой информации, он вправе получать эти данные только с письменного согласия работника и при условии, что эта информация непосредственно связана с трудовыми отношениями.

На практике часто возникает вопрос: «относится ли фотография работника к персональным данным?» В действующем законодательстве прямо не установлено, что фотография относится к персональным данным. Однако работодатель не может использовать фотографию работника без его согласия. Исходя из определения персональных данных, которое дано в Законе о персональных данных, затруднительно сказать, является ли фотография сама по себе персональными данными. Как следует из редакции Закона «О персональных данных», под персональными данными понимается информация, которая относится прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных). В этом Законе фотография прямо не указана как объект, на основании которого можно идентифицировать человека (п. 1 ст. 3 Закона о персональных данных). Следовательно, отнести ее к персональным данным, вероятнее всего, нельзя [24].

Тем не менее, согласно ст. 152.1 ГК РФ обнародование и дальнейшее использование изображения гражданина допускаются только с его согласия. Соответственно, использование фотографии человека (в том числе работника) без его согласия не допускается.

1.3. Виды персональных данных

Персональные данные исключительно разнообразны и разнородны. Их можно по-разному объединять в различные группы в зависимости от избранного критерия и цели классификации, классифицировать. Любая классификация будет достаточно условной, так как некоторые сведения могут в равной степени относиться сразу к нескольким группам. Поэтому правовое регулирование такого сложного института, как институт персональных данных, должно быть многовариантным и гибким.

Законодательство определяет различные категории (виды) персональных данных. К ним могут относиться: общедоступные

персональные данные, специальные категории персональных данных, категории персональных данных, обрабатываемые в информационных системах персональных данных, биометрические персональные данные и другие. В этой классификации персональные данные объединены в группы в зависимости от правового режима их оборота, определяемого различными методами правового регулирования.

1) Общедоступные персональные данные

Общедоступными являются персональные данные, доступ к которым предоставлен неограниченному кругу лиц с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяются требования соблюдения конфиденциальности (п.12 ст.3 Закона о персональных данных). Такие данные могут включать фамилию, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные. Источниками такой информации являются, к примеру, справочники, адресные книги и т.п.

Сведения о субъекте персональных данных могут быть исключены из общедоступных источников в любое время по требованию субъекта либо по решению суда или уполномоченных государственных органов.

2) Специальные категории персональных данных

Специальные категории ПД представляют собой особую группу персональных данных. К специальным категориям относятся персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, философских или религиозных убеждений, интимной жизни, состояния здоровья (ст.10 ФЗ «О персональных данных»). Информация специального характера может потребоваться при трудоустройстве на новое место работы.

Их обработка допускается только в определенных Законом случаях. Обработка специальных категорий персональных данных, должна быть незамедлительно прекращена, если устранены причины, вследствие которых осуществлялась обработка, если иное не установлено федеральным законом.

3) Категории персональных данных, обрабатываемых в информационных системах персональных данных.

Совместный приказ ФСТЭК, ФСБ и Министерства информационных технологий и связи РФ от 13 февраля 2008 года N 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных» устанавливает следующие категории персональных данных, которые подвергаются обработке в информационных системах персональных данных:

Категория 1 – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, философских или религиозных убеждений, интимной жизни, состояния здоровья .

Категория 2 – персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к категории 1.

Категория 3 – персональные данные, позволяющие идентифицировать субъекта персональных данных.

Категория 4 – обезличенные и (или) общедоступные персональные данные.

4) Биометрические персональные данные

Биометрические персональные данные – это сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность. Биометрические персональные данные обрабатываются в соответствии со статьей 11 Федерального закона Российской Федерации от 27 июля 2006 г. N 152-ФЗ «О персональных данных» [29].

Они могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных. Обработка биометрических персональных данных без согласия субъекта персональных данных может осуществляться в связи с осуществлением правосудия, а также в случаях,

предусмотренных законодательством Российской Федерации о безопасности, о государственной службе, об оперативно-розыскной деятельности, о порядке выезда из РФ и въезда в Российскую Федерацию, уголовно-исполнительным законодательством.

Исходя из определения биометрических персональных данных, к ним относятся физиологические параметры (анализы ДНК, дактилоскопические данные, радужная оболочка глаз, вес, рост и др.), а также иные биологические или физиологические характеристики человека, в том числе его изображения (видеозапись и фотография), которые позволяют установить личность субъекта и с этой целью используются оператором (Разъяснения Роскомнадзора «О вопросах отнесения фото- и видео- изображения, дактилоскопических данных и иной информации к биометрическим персональным данным и особенностям их обработки»). Это подтверждают и представители регуляторов, в частности Федеральной службы по техническому и экспортному контролю. Фотографии субъектов персональных данных могут обрабатываться в пропускных системах и системах контроля доступа, видеоизображения – в системах видеонаблюдения и т.п.

Биометрические персональные данные могут обрабатываться оператором только при наличии письменного согласия субъекта персональных данных (за исключением случаев, установленных в ч. 2 ст. 11 Закона). Согласие на обработку биометрической персональной информации чаще всего необходимо оформлять для проведения медицинского обследования или лечения [18].

Наиболее логичной и ориентированной на правоприменителя представляется группировка персональных данных по признаку свободы оборота. Эта классификация уже частично сложилась и используется на уровне обычая. Исходя из этого персональные данные можно разделить на:

- свободно обрабатываемые персональные данные - имя, фамилия, отчество и пол лица. В некоторых случаях к ним можно добавить адрес места жительства, возраст, номер телефона, образование, т.е. все те минимальные сведения, которые готов сообщить о себе субъект определенному кругу лиц и организаций, составляющих круг его ежедневного социального общения. Как правило, несанкционированное использование этих сведений не может причинить субъекту какого-либо существенного вреда, поэтому применение мер ответственности возможно только в том случае, если нарушен порядок сбора и обработки этой информации (в частности, должностным лицом).

- ограниченно обрабатываемые персональные данные - различные виды персональных данных, в том числе и данные регистрационных номеров документов, сообщаемые субъектом (с его согласия) различным организациям и органам с целью получения каких-либо услуг или совершения каких-либо действий. Разглашение или иное несанкционированное использование полученных персональных данных это грубое нарушение неприкосновенности частной жизни субъекта персональных данных, способное причинить ему материальный и моральный ущерб. Субъектами мер ответственности в этом случае будут выступать преимущественно должностные лица, что будет влиять на тяжесть применяемых мер ответственности.

- персональные данные, обрабатываемые в специальных целях - те персональные данные, в том числе биометрические, которые собираются государственными, муниципальными и иными уполномоченными органами в рамках их полномочий в соответствии с законодательством. Согласие субъекта на сбор этих персональных данных требуется не всегда. К таким сведениям относится, например, информация об усыновлении. Разглашение и иное несанкционированное использование этих данных должно влечь за собой жесткие меры ответственности.

- запрещенные к обороту персональные данные - специальные категории персональных данных. За нарушения положений законодательства

о защите специальных категорий персональных данных должны устанавливаться наиболее жесткие меры ответственности, вплоть до уголовной ответственности [25].

Также существует еще классификация персональных данных, которые находятся у работодателя (по стадии получения персональных данных):

1) сведения, представляемые работником при приеме на работу, предусмотренные в ст. 65 Трудового кодекса РФ (сведения, содержащиеся в паспорте или ином документе, удостоверяющем личность работника; сведения об образовании, квалификации; сведения, имеющиеся в трудовой книжке; сведения, содержащиеся в документах медицинского освидетельствования работника, и др.);

2) сведения, создаваемые и получаемые работодателем в период трудовой деятельности работника (сведения, содержащиеся в личном деле работника, в приказах, характеристиках, распоряжениях, аттестационных материалах, и др.);

3) сведения о работнике, хранящиеся у работодателя после прекращения с ним трудовых отношений (все персональные данные работника, имеющиеся в архиве организации) [53].

Как уже отмечалось, любая классификация персональных данных является в известной мере условной. В Законе затруднительно учесть все возможные варианты и случаи сбора персональных данных и закрепить перечни для каждого конкретного случая. Но дальнейшая работа в этом направлении необходима, так как на основе различных классификаций персональных данных можно установить дифференцированную систему мер ответственности за нарушение законодательства о персональных данных, а также использовать их при разработке подзаконных нормативных актов. Такой подход, будет способствовать как развитию законодательства, так и эффективной защите прав субъектов персональных данных.

2. Правовое содержание защиты персональных данных работника

2.1. Обработка персональных данных работника

Любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных называется обработкой персональных данных (ст. 3 Закона N 152-ФЗ) [7].

Согласно статье 86 Трудового кодекса РФ обработка персональных данных работника может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, обучении и продвижении по службе, содействия работникам в трудоустройстве, контроля количества и качества выполняемой работы и обеспечения сохранности имущества, обеспечения личной безопасности работников [4]. Другими словами, получение и обработка персональных данных должны проводиться только в целях обеспечения трудовых прав и законных интересов работников и работодателей.

Запрет получать информацию в иных целях и в большем объеме, чем предусмотрено Конституцией РФ и федеральными законами приобретает особое значение. При этом работодатель не имеет права получать и обрабатывать сведения о работнике, относящиеся к специальным категориям персональных данных, а также данные о членстве работника в общественных объединениях или о его профсоюзной деятельности, за исключением случаев, предусмотренных законодательством.

В ряде случаев работники по своей инициативе либо по требованию работодателя представляют о себе дополнительные сведения, не

предусмотренные ТК РФ или иными федеральными законами. В этом случае, если эти сведения не имеют отношения к будущей трудовой функции работника и являются лишними по отношению к целям сбора персональных данных, работодатель не имеет права их обрабатывать.

Все персональные данные следует получать от самого работника. Если же их можно получить только у третьей стороны, то работника нужно уведомить об этом заранее и получить от него письменное согласие. Кроме того, работодатель должен сообщить работнику о целях, предполагаемых способах и источниках получения персональных данных, а также о характере подлежащих получению данных и последствиях отказа работника согласиться на их получение.

Работодатель устанавливает в локальном акте порядок обработки персональных данных, а также права и обязанности работников в этой области, с этим документом работники должны быть ознакомлены под роспись.

Работники не должны отказываться от своих прав на сохранение и защиту тайны. Работодатели, работники и их представители должны совместно вырабатывать меры защиты персональных данных работников [54].

Меры по обеспечению безопасности персональных данных при их обработке установлены ст. 19 Закона N 152-ФЗ. Требования к защите этих данных при их обработке в информационных системах установлены Постановлением Правительства РФ от 01.11.2012 N 1119, а Постановлением Правительства РФ от 15.09.2008 N 687 утверждено Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации.

Обработка персональных данных осуществляется с согласия работника, и получить данное согласие необходимо при приеме на работу. Согласие предоставляется субъектом персональных данных свободно, своей волей и в своем интересе. Дать согласие на обработку данных может и представитель

субъекта персональных данных, но в этом случае обязательно должен быть документ, подтверждающий полномочия данного представителя давать согласие от имени субъекта (доверенность).

Обязанность предоставить доказательства наличия согласия субъекта персональных данных на их обработку возлагается на оператора.

Согласно ст. 9 Закона N 152-ФЗ согласие на обработку персональных данных должно быть конкретным, информированным и сознательным. Так, согласно постановлению Федерального арбитражного суда Северо-Западного округа от 13 мая 2009 г. по делу № А66-17/2009, в одном деле оператор услуг телефонной связи был привлечен к административной ответственности за то, что в типовом договоре на оказание услуг междугородной и международной телефонной связи был определен только порядок предоставления данных услуг, но отсутствовало непосредственное указание о согласии или отказе абонента на доступ к указанным услугам и на предоставление сведений о нем третьим лицам.

Согласие в письменной форме субъекта персональных данных на обработку его персональных данных должно включать в себя, в частности (ч. 4 ст. 9 Закона N 152-ФЗ):

- фамилия, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

Речь идет о работнике, персональные данные которого подлежат обработке. В согласии должно быть указаны все выше предусмотренные координаты.

- фамилия, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);

Речь идет о представителе работника, персональные данные которого подлежат обработке. В согласии должно быть указаны все выше предусмотренные координаты. В частности, такая ситуация может возникнуть, когда в соответствии с ч. 4 ст. 63 ТК РФ трудовой договор от имени лица, не достигшего возраста 14 лет, подписывается его родителем (опекуном).

- наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта персональных данных;

Данный пункт в качестве оператора рассматривает работодателя; Наименование организации работодателя указывается в соответствии с учредительными документами организации. Фамилия, имя, отчество уполномоченного лица, адрес местонахождения организации.

- цель обработки персональных данных;

В соглашении необходимо указать все цели, для которых берется письменное согласие работника. В качестве целей могут быть заявлены: публичное обращение, указание на сайте компании, на странице доступной только для работников, указание во внутреннем телефонном справочнике компании, указание под фотографией на доске почета, внесение в бухгалтерские информационные системы работодателя, для публичного поздравления с днем рождения, с юбилеями, для отражения этой информации в кадровых документах, для предоставления льгот, установленных действующими нормами законодательства, например при сокращении численности и других кадровых процедурах, для расчета страхового стажа на оплату листов нетрудоспособности и т.д.

- перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

В соглашении необходимо указать все персональные данные, для обработки которых берется письменное согласие работника. Это могут быть следующие персональные данные: фамилия, имя, отчество, дата, месяц, год рождения, семейное положение, предыдущие места работы\службы (с

указанием периодов, места работы/ службы, должностей), ближайшие родственники, квалификация, образование, профессия, фактический адрес места жительства и т.д.

- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка будет поручена такому лицу;

В случае обработки персональных данных работников организации другим лицом, по поручению работодателя - письменная форма согласия должна содержать координаты (фамилию, имя, отчество и адрес) лица, которое будет осуществлять такую обработку.

- перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;

Поскольку обработка персональных данных осуществляется как на бумажных носителях, так и в электронном виде, то указать необходимо весь перечень действий с персональными данными и способы обработки.

- срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;

Работник сам определяет, на какой срок он разрешает производить обработку своих персональных данных. Срок необходимо определять, руководствуясь требованиями архивного законодательства (Перечнем типовых документов, образующихся в деятельности госкомитетов, министерств, ведомств и других учреждений, предприятий, организаций с указанием сроков хранения) после завершения которого персональные данные работника должны быть уничтожены.

- подпись субъекта персональных данных. Письменная форма согласия должна содержать подпись работника. После подписанных работниками соглашений работодатель приступает к обработке персональных данных представленных в согласиях [20].

Согласие на обработку персональных данных может быть отозвано их субъектом. Однако в случаях, установленных Законом N 152-ФЗ, обработка может осуществляться и без согласия работника.

Действие Закона о персональных данных не распространяется на отношения, возникающие при:

- обработке персональных данных физическими лицами исключительно для личных и семейных нужд, если при этом не нарушаются права субъектов персональных данных;

- организации хранения, комплектования, учета и использования содержащих персональные данные документов Архивного фонда Российской Федерации и других архивных документов в соответствии с законодательством об архивном деле в Российской Федерации (Положение Федерального закона от 22 октября 2004 г. N 125-ФЗ «Об архивном деле в Российской Федерации»);

- обработке персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну (ст. 9 Закона Российской Федерации от 21 июля 1993 г. N 5485-1 «О государственной тайне»);

- предоставлении уполномоченными органами информации о деятельности судов в Российской Федерации в соответствии с Федеральным законом от 22 декабря 2008 г. N 262-ФЗ «Об обеспечении доступа к информации о деятельности судов в Российской Федерации»;

- обработка биометрических персональных данных в связи с реализацией международных договоров Российской Федерации о реадмиссии, в связи с осуществлением правосудия и исполнением судебных актов, а также в случаях, предусмотренных законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-розыскной деятельности, о государственной службе, уголовно-исполнительным законодательством Российской Федерации, законодательством Российской Федерации

Федерации о порядке выезда из Российской Федерации и въезда в Российскую Федерацию, о гражданстве Российской Федерации .

Глава 2 Закона о персональных данных носит название «Принципы и условия обработки персональных данных». Статья 5 Закона о персональных данных регламентирует принципы обработки персональных данных:

1. Обработка персональных данных должна осуществляться на законной и справедливой основе.

2. Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

Целевой характер означает, что персональные данные должны храниться не дольше, чем этого требует цель, для которой они накапливаются, и подлежат уничтожению, если в них отсутствует надобность. В Трудовом кодексе РФ не закреплены ни правила об ограничении сроков их хранения, ни конкретные цели обработки персональных данных.

3. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

4. Обработке подлежат только персональные данные, которые отвечают целям их обработки.

5. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

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

7. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

Согласно статье 6 Закона о персональных данных, которая регламентирует условия обработки персональных данных - обработка персональных данных должна осуществляться с соблюдением принципов и правил, предусмотренных настоящим Федеральным законом [7].

Работодатель вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия государственным или муниципальным органом соответствующего акта. Лицо, осуществляющее обработку персональных данных по поручению Работодателя, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом «О персональных данных».

В поручении Работодателя должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных.

Лицо, осуществляющее обработку персональных данных по поручению Работодателя, не обязано получать согласие субъекта персональных данных на обработку его персональных данных. В случае, если Работодатель поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет Работодатель. Лицо, осуществляющее обработку персональных данных по поручению Работодателя, несет ответственность перед Работодателем [20].

Обработка персональных данных может осуществляться с использованием и без использования средств автоматизации.

1) обработка персональных данных без использования средств автоматизации

Порядок обработки персональных данных, осуществляемой без использования средств автоматизации, может устанавливаться федеральными законами и иными нормативными правовыми актами РФ.

В настоящее время действует Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденное Постановлением Правительства РФ от 15.09.2008 N 687.

Пункт 6 Постановления Правительства РФ от 15.09.2008 N 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» гласит, что лица, осуществляющие обработку персональных данных без использования средств автоматизации, должны быть проинформированы о факте обработки персональных данных.

Согласно данному Положению обработкой персональных данных без применения средств автоматизации считаются использование, распространение, уточнение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, которые осуществляются при непосредственном участии человека. При

использовании типовых форм в работе, необходимо соблюдать установленные постановлением требования [55].

2) обработка персональных данных с использованием средств автоматизации

Под автоматизированной обработкой персональных данных понимаются действия, которые выполняются без участия человека, т.е. полностью автоматически. Обработка персональных данных не может быть признана осуществляемой с использованием средств автоматизации только на том основании, что эти данные содержались в информационной системе персональных данных либо были извлечены из нее.

Уполномоченный представитель работодателя обрабатывает персональные данные работников. Уполномоченный должен руководствоваться правилами, предусмотренными для обработки персональных данных без использования средств автоматизации.

Особенности обработки персональных данных в информационных системах:

- определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

- применение технических и организационных мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные правительством Российской Федерации уровни защищенности персональных данных;

- применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

- оценка эффективности принимаемых мер по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных;

- учет машинных носителей персональных данных;

- обнаружение фактов несанкционированного доступа к персональным данным и принятием мер;
- восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- установление правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;
- контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных [28].

Кроме того, работодатель в процессе своей деятельности собирает информацию о кандидатах на трудоустройство, соискателях, необходимую для принятия решения о вступлении с ними в трудовые отношения. Если эта информация содержит персональные данные кандидатов, к ней в полной мере относятся установленные законом требования о сборе, обработке, защите, хранении персональных данных.

2.2. Хранение, использование и передача персональных данных работников

Работодатель осуществляет использование, хранение и передачу персональных данных в строгом соответствии с требованиями законодательства. Доступ к персональным данным работников должен осуществляться только специально уполномоченными лицами, при этом они имеют право получать лишь те данные работника, которые необходимы для выполнения конкретных функций.

Согласно ст. 87 ТК РФ порядок хранения и использования персональных данных работников устанавливается работодателем с соблюдением требований Трудового кодекса и иных федеральных законов.

Соответствующие нормы могут быть включены в локальный акт организации о персональных данных. При этом они должны отвечать требованиям, установленным ТК РФ и иными федеральными законами [4].

В целях защиты персональных данных со стороны работодателя он должен в первую очередь обеспечить их хранение. Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

В соответствии с п. 13, 15 Постановления Правительства РФ от 15.09.2008 N 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

При хранении материальных носителей должны соблюдаться условия, которые обеспечат сохранность персональных данных и исключат несанкционированный к ним доступ. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются оператором [18].

Хранение персональных данных работников осуществляется работодателем в документированной форме, в том числе в форме электронного документа. В настоящее время для целей хранения персональных данных работников применяется личная карточка работника, оформляемая по унифицированной форме Т-2, утвержденной постановлением Госкомстата России от 5 января 2004 г. № 1 «Об утверждении унифицированных форм первичной учетной документации по учету труда и его оплаты».

Персональные данные работников содержатся и в иных документах, в первую очередь - в приказах по личному составу, которые оформляются при приеме, переводе, увольнении работников, а также в иных случаях, требующих издания правоприменительного акта.

На работников могут вестись личные дела, к которым приобщаются документы, содержащие персональные данные. В настоящее время требования об обязательном ведении личных дел распространяются лишь на государственных и муниципальных служащих, прокурорских работников, судей. Остальные работодатели могут самостоятельно принимать решения о необходимости ведения личных дел работников и определять порядок их ведения, в том числе устанавливать перечень документов, приобщаемых к личному делу работника. При этом работодатель обязан соблюдать требования законодательства, предъявляемые к обработке и защите персональных данных работников [19].

В соответствии с федеральным законом «О персональных данных» хранение персональных данных работников должно осуществляться не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом.

В настоящее время срок хранения документированной информации, содержащей персональные данные работников, определен, в соответствии с Федеральным законом от 22 октября 2004 г. № 125-ФЗ «Об архивном деле в Российской Федерации», приказом Минкультуры России от 25 августа 2010 г. № 558 «Об утверждении Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения».

В частности, в нем, определены следующие сроки хранения документов, содержащих персональные данные работников:

- приказы по личному составу о приеме, увольнении, перемещении, переводе работников, направлении их на повышение квалификации, об

изменении фамилии, поощрении, предоставлении всех видов отпусков работникам с тяжелыми, вредными и опасными условиями труда, предоставлении отпусков по уходу за ребенком, отпусков без сохранения заработной платы, о направлении работников в длительные внутрироссийские и зарубежные командировки, а также о направлении в служебные командировки работников с тяжелыми, вредными и опасными условиями труда -75 лет;

- трудовые договоры с работниками -75 лет;

- личные карточки работников —75 лет;

- личные дела работников —75 лет;

- приказы о применении дисциплинарных взысканий, о предоставлении ежегодных оплачиваемых и учебных отпусков (за исключением случаев, когда данные отпуска предоставляются работникам с тяжелыми, вредными и опасными условиями труда), о направлении в краткосрочные внутрироссийские и зарубежные командировки (кроме случаев направления в служебные командировки работников с тяжелыми, вредными и опасными условиями труда) - 5 лет;

- личные дела руководителей организации, членов руководящих, исполнительных, контрольных органов организации, членов (депутатов) представительных органов РФ, субъектов РФ, органов местного самоуправления, работников, имеющих государственные и иные звания, премии, награды, степени и звания - постоянно;

- подлинные личные документы (в первую очередь - трудовые книжки работников) - до востребования (невостребованные хранятся 75 лет).

Столь длительные сроки хранения документов обеспечивают право граждан на доступ к своим персональным данным, в том числе и после прекращения трудового договора, а также гарантируют возможность доказать различные факты своей трудовой биографии, например, подтвердить страховой стаж для установления трудовой пенсии. С другой стороны, длительные сроки хранения документов предъявляют повышенные

требования к защите персональных данных работников от несанкционированного доступа или утраты.

Поскольку в процессе трудовой деятельности возникает необходимость передавать персональные данные работника как внутри организации, так и третьим лицам, должен вестись их строгий учет.

Передача персональных данных работника является одной из разновидностей обработки персональных данных. Данный процесс регулируется ст. 88 Трудового кодекса РФ. При передаче персональных данных работника работодатель должен соблюдать следующие требования:

- 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 ТК РФ или иными федеральными законами.

Здесь следует обратить внимание на то, что работодатель в данном случае самостоятельно оценивает степень угрозы жизни и здоровью работника и с целью предупреждения такой угрозы предоставляет персональную информацию третьим лицам. Примером данного положения может быть указание ст. 228 Трудового кодекса РФ о незамедлительном информировании при несчастном случае родственников пострадавшего работника, а также ряд государственных и местных властных структур.

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

- предупредить лиц, которые получают 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. Лица, которые получают персональные данные работника, обязаны соблюдать режим секретности (конфиденциальности). Отметим, что данное положение не распространяется на обмен

персональными данными работников в порядке, установленном ТК РФ и иными федеральными законами;

- 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 эти 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 ТК РФ и иными федеральными законами, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций [4].

Основанием для передачи персональных данных работника является письменный запрос от должностного лица соответствующего государственного органа, а если представители контролирующих органов пришли лично - служебное удостоверение и приказ, где указаны цели сбора подобной информации.

Работодатель должен обеспечить ведение журнала учета выданных персональных данных работников, в котором регистрируются запросы, фиксируются сведения о лице, направившем запрос, дата передачи персональных данных или дата уведомления об отказе в предоставлении персональных данных, а также отмечается, какая именно информация была передана.

Если лицо, которое обратилось с запросом, не уполномочено федеральным законом на получение персональных данных работника либо отсутствует письменное согласие работника на предоставление его персональных сведений, работодатель обязан отказать в предоставлении персональных данных. Лицу, который обратился с запросом, выдается письменное уведомление об отказе в предоставлении персональных данных [21].

2.3. Права работника как субъекта персональных данных

Европейская конвенция о защите физических лиц при автоматизированной обработке персональных данных гарантирует, что любому лицу при обработке его персональных данных должна быть предоставлена возможность:

- знать о существовании автоматизированной базы персональных данных;
- знать основные цели автоматизированной базы персональных данных;
- знать сведения об организации, наделенной полномочиями решать, для какой цели создается автоматизированная база данных, какие категории персональных данных будут накапливаться, какие способы обработки персональных данных будут применяться;
- получать по запросу в разумный срок и без чрезмерных затрат денежных средств подтверждение того, хранятся ли касающиеся его персональные данные в автоматизированной базе данных, а также получить доступ к своим персональным данным, представленным в доступной для понимания форме;
- добиваться в случае необходимости уточнения или уничтожения таких данных, если они обрабатывались с нарушением закона;
- получить судебную защиту нарушенного права в случае отказа в предоставлении подтверждения обработки персональных данных в

автоматизированной базе данных, в доступе к своим персональным данным (за исключением случаев ограничения доступа к персональным данным в целях защиты безопасности государства и общественного порядка), а также отказа в их изменении или уничтожении [37].

Права работников, предусмотренные трудовым законодательством в целях защиты их персональных данных, хранящихся у работодателя, повторяют и дополняют положения Конвенции. Права работников в целях обеспечения защиты персональных данных, которые хранятся у работодателя, регламентированы ст. 89 ТК РФ.

Так, в целях обеспечения защиты персональных данных, хранящихся у работодателя, работники имеют право на:

- полную информацию об их персональных данных и обработке. ЛНА должен содержать информацию о том, какие персональные данные работников, кем и с какой целью обрабатываются внутри организации;

- свободный бесплатный доступ к своим персональным данным, включая в том числе право на получение копий любой записи, содержащей персональные данные работника, за исключением случаев, предусмотренных федеральным законом (ограничения в доступе установлены ч. 8 ст. 14 Закона N 152-ФЗ). В соответствии со ст. 62 ТК РФ, по письменному заявлению работника работодатель обязан не позднее трех рабочих дней со дня подачи данного заявления безвозмездно выдать работнику надлежащим образом заверенные копии документов, которые связаны с работой. К таким копиям, в частности, относятся копии приказов; выписки из трудовой книжки; о начисленных и фактически уплаченных страховых взносах на обязательное пенсионное страхование, справки о заработной плате, о периоде работы и др.

Если кадровый документ содержит персональные данные нескольких лиц, доступ к нему одного из этих лиц возможен только с согласия остальных. При отсутствии такого согласия работнику может быть предоставлена выписка из документа;

- определение своих представителей для защиты своих персональных данных. Работник может выдать доверенность представителю, который вправе от его имени обращаться к работодателю, например с досудебным требованиям: прекратить обработку ПД, и с любым иным требованием, полномочия на которые переданы по соответствующей доверенности;

- доступ к медицинской документации, которая отражает состояние их здоровья, с помощью медицинского работника по их выбору;

- требование об исключении либо исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований ТК РФ или иного федерального закона. При отказе работодателя исключить или исправить персональные данные работника он имеет право заявить в письменной форме работодателю о своем несогласии с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера работник имеет право дополнить заявлением, которое будет выражать его собственную точку зрения;

- 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 [4].

Отказ работников от своих прав на защиту персональных данных юридически ничтожен. Обязанности работников в области обработки персональных данных не предусмотрены Трудовым законодательством. Также, законодательно не закреплена обязанность работников сообщать работодателю обо всех изменениях в их персональных данных. Однако сокрытие работником сведений, способных повлиять на принимаемые работодателем решения в отношении данного работника, впоследствии могут быть расценены как злоупотребление правом со стороны работника.

В п. 27 постановления Пленума Верховного Суда РФ от 17 марта 2004г. № 2 выделяется необходимость соблюдения общеправового принципа

недопустимости злоупотребления правом, в том числе и со стороны самих работников. В частности, обращается внимание на недопустимость сокрытия работником того обстоятельства, что он является членом профессионального союза или руководителем (его заместителем) выборного коллегиального органа первичной профсоюзной организации, выборного коллегиального органа профсоюзной организации СП организации (не ниже цехового и приравненного к нему), не освобожденным от основной работы, в тех случаях когда решение вопроса об увольнении должно производиться с соблюдением процедуры учета мотивированного мнения выборного органа первичной профсоюзной организации либо соответственно с предварительного согласия вышестоящего выборного профсоюзного органа.

При установлении судом факта злоупотребления работником правом суд может отказать в удовлетворении его иска о восстановлении на работе, поскольку в указанном случае работодатель не должен отвечать за неблагоприятные последствия, наступившие вследствие недобросовестных действий со стороны работника.

2.4. Ответственность за нарушение порядка работы с персональными данными

К ответственности за нарушение положений законодательства РФ в области персональных данных при обработке персональных данных работника могут быть привлечены как работодатели, так и конкретные должностные лица, у которых в трудовых функциях вменена обработка персональных данных работников.

В соответствии с действующим законодательством, на основании ст. 90 ТК РФ, лица виновные в нарушении положений законодательства Российской Федерации в области персональных данных при обработке персональных данных работника привлекаются к следующим видам ответственности:

- дисциплинарной;

- материальной;
- гражданско-правовой;
- административной;
- уголовной.

Но привлечь должностное лицо к ответственности можно только при наличии обязательства о неразглашении таких сведений. На данное обстоятельство Пленум ВС РФ обратил внимание в п. 43 Постановления от 17.03.2004 N 2. Поэтому при наделении должностного лица полномочиями на доступ к персональным данным других работников (их сбор, обработку и передачу третьим лицам) одновременно с таким лицом необходимо оформить еще и обязательство (в произвольной форме) о неразглашении указанной информации.

Рассмотрим каждый вид ответственности в отдельности и подробно.

1) Дисциплинарная ответственность

Дисциплинарная ответственность применяется к работникам, нарушившим нормы законодательства в области персональных данных, в порядке, предусмотренном ТК РФ.

За дисциплинарный проступок сбора, обработки и хранения персональных данных работодатель может наказать своего работника, применив к нему одно из следующих взысканий (ч.1 ст. 192 ТК РФ): замечание; выговор; увольнение.

В соответствии со ст. 192 ТК РФ привлечение работника, совершившего дисциплинарный проступок, является правом, а не обязанностью работодателя. При наложении дисциплинарного взыскания работодатель должен учесть тяжесть совершенного проступка и обстоятельства, при которых он был совершен.

Права и обязанности работника в отношении доступа к персональным данным других работников определяются его трудовой функцией, другими условиями трудового договора, а также содержанием локальных

нормативных правовых актов, определяющих перечень его должностных обязанностей.

При привлечении к дисциплинарной ответственности в виде увольнения для работника, разгласившего охраняемую законом тайну (в том числе персональные данные другого работника), необходимо, чтобы эти сведения стали известны работнику в связи с исполнением им своих трудовых обязанностей (под, «в» п. 6 ст. 81 ТК РФ). Для применения ответственности этого вида необходимо доказать сам факт разглашения персональных данных должностным лицом [4].

В соответствии с п. 43 постановления Пленума Верховного Суда РФ от 17 марта 2004 г. № 2 в случае оспаривания работником увольнения по подп. «в» п. 6 ч. 1 ст. 81 ТК РФ работодатель обязан представить доказательства, свидетельствующие о том:

- что сведения, разгласившие работником в соответствии с действующим законодательством относятся к государственной, коммерческой, служебной, или иной охраняемой законом тайне, либо к персональным данным другого работника;

- работнику эти сведения стали известны в связи с исполнением им его трудовых обязанностей;

- он обязывался не разглашать данные сведения.

Рассмотрим один из примеров судебной практики по вопросу увольнения работника, который разгласил персональные данные другого работника - Апелляционное определение Иркутского областного суда от 19.09.2013 по делу N 33-7662/2013.

Рассматривая дело, суд принял решение, что наличие у работника возможности получения какой-либо информации о работниках организации не свидетельствует о факте получения им данной информации именно в связи с исполнением своих трудовых функций и не подтверждает обстоятельство получения истцом информации о других работниках в связи с исполнением Колмаковым своих трудовых обязанностей.

Доказательства, бесспорно свидетельствующие о факте получения истцом информации персональных данных другого работника в связи с исполнением Колмаковым трудовой функции, в материалах дела отсутствовали.

Судебная коллегия пришла к выводу, что ответчиком, на которого в силу положений ст. 56 ГК РФ возлагается бремя доказывания законности увольнения истца, наличие в совокупности условий, позволяющих произвести увольнение работника на основании подп. «в» п. 6 ч. 1 ст. 81 ТК РФ, не доказано.

При таких обстоятельствах выводы суда о законности увольнения работника Колмакова Е.А. нельзя признать правильными, в связи с чем решение суда в части отказа истцу в удовлетворении исковых требований о признании незаконным приказа о привлечении к дисциплинарной ответственности, приказа об увольнении, признании незаконными увольнения и записи в трудовой книжке, восстановлении на работе, взыскании среднего заработка за время вынужденного прогула, компенсации морального вреда подлежит отмене.

Таким образом, апелляционная жалоба работника Колмакова подлежала удовлетворению, решение суда в части отказа в удовлетворении требований Колмакова Е.А. о признании незаконными приказа о привлечении к дисциплинарной ответственности, приказа об увольнении, признании незаконными увольнения и записи в трудовой книжке, восстановлении на работе, взыскании среднего заработка за время вынужденного прогула, компенсации морального вреда подлежали отмене [56].

Таким образом, приказ об увольнении за однократное грубое нарушение работником трудовых обязанностей - разглашение персональных данных работника, ставших известными работнику в связи с исполнением им трудовых обязанностей, подпункт «в» пункта 6 части 1 статьи 81 ТК РФ был признан незаконным, работник восстановлен на работу.

2) Материальная ответственность

Что касается материальной ответственности как самого работодателя, так и конкретных должностных лиц, то она может наступить в случае причинения работнику материального ущерба нарушением норм о защите его персональных данных.

Также подлежит возмещению в соответствии с законодательством РФ моральный вред, причиненный работнику вследствие нарушения прав правил обработки и требований к защите персональных данных. В случае незаконного распространения информации о персональных данных работнику может быть причинен моральный вред. Работник вправе потребовать возмещения морального вреда от работодателя. Последний впоследствии может взыскать его с непосредственного виновного лица (ст. ст. 238, 248 ТК РФ).

Из судебной практики апелляционного определения Верховного суда Республики Саха (Якутия) от 23.10.2013 по делу N 33-4172/13 - работник просил признать незаконными действия организации по разглашению персональных данных, а именно размещение на сайте статьи с приложением текста дополнительного соглашения к трудовому договору данного работника. Свои требования он подтвердил протоколом осмотра доказательств (сайта), составленного нотариусом. Суд удовлетворил требования истца, и указал, что в результате нарушения работодателем норм защиты персональных данных работника для последнего наступили негативные последствия: условия трудового договора стали предметом обсуждения неограниченного числа пользователей всемирной сети Интернет [57].

При этом, если выплаты в пользу работника, права которого были нарушены, были произведены работодателем, то при определенных обстоятельствах на должностных лиц, которые допустили нарушения законодательства в области защиты и обработки персональных данных,

может быть возложена полная материальная ответственность в порядке, предусмотренной гл. 39 ТК РФ [45].

Материальная ответственность работника за разглашение сведений, которые относятся к персональным данным других работников, возлагается на него в полном размере причиненного ущерба (п. 7 ст. 243 ТК РФ). Случаи полной материальной ответственности являются исключениями из общего правила, что еще раз подтверждает особое значение института защиты персональных данных работников в отечественном трудовом праве.

Работодатель применяет дисциплинарную и материальную ответственность исключительно по своему усмотрению. Государственные контролирующие органы (в том числе Роскомнадзор) в данном процессе участия не принимают [47].

3) Гражданско-правовая ответственность

Статьей 17 Федерального закона от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» предусмотрено, что лица, права и законные интересы которых были нарушены в связи с разглашением информации ограниченного доступа или иным ее неправомерным использованием, могут обратиться в установленном порядке за судебной защитой своих прав, в том числе с исками о возмещении убытков, компенсации морального вреда, защите чести, достоинства и деловой репутации.

Статья 150 ГК РФ к числу неотъемлемых и неотчуждаемых нематериальных прав, которые подлежат правовой защите, относит личную неприкосновенность, неприкосновенность частной жизни, личную и семейную тайну. Гражданско-правовая ответственность за посягательство на неприкосновенность частной жизни непосредственно связана с категорией морального вреда. Если гражданину причинен моральный вред (физические или нравственные страдания) действиями, нарушающими его личные неимущественные права либо посягающими на принадлежащие гражданину другие нематериальные блага, а также в других случаях, предусмотренных

законом, суд может возложить на нарушителя обязанность денежной компенсации указанного вреда [27].

При определении размеров компенсации морального вреда суд принимает во внимание степень вины нарушителя и иные обстоятельства, которые заслуживают внимания. Суд должен также учитывать степень физических и нравственных страданий, связанных с индивидуальными особенностями лица, которому причинен вред (ст. 151 ГК РФ). Кроме того, гражданин вправе требовать по суду опровержения порочащих его честь, достоинство или деловую репутацию сведений, если распространивший такие сведения не докажет, что они соответствуют действительности.

Разъяснения вопросов, связанных с причинением морального вреда, содержатся в постановлении Пленума Верховного Суда РФ от 20 декабря 1994 г. № 10 «Некоторые вопросы применения законодательства о компенсации морального вреда». Компенсация морального вреда осуществляется в денежной форме. Характер физических и нравственных страданий оценивается судом с учетом фактических обстоятельств, при которых был причинен моральный вред, и индивидуальных особенностей потерпевшего (ст. 1101 ГК РФ).

4) Уголовная ответственность (применяется в случаях превышения должностными лицами работодателя своих полномочий по доступу к информации о частной жизни работника):

- незаконные сбор или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации (ст. 137 УК РФ предусматривает ответственность за нарушение неприкосновенности частной жизни).

В связи с тем, что хранение персональных данных работников осуществляется работодателем, в том числе в форме электронных

документов, им должны приниматься меры по защите информации от несанкционированного доступа или утраты.

- неправомерный отказ должностного лица в предоставлении собранных в установленном порядке документов и материалов, непосредственно затрагивающих права и свободы гражданина, либо предоставление гражданину неполной или заведомо ложной информации, если эти деяния причинили вред правам и законным интересам граждан (ст. 140 УК РФ);

- неправомерный доступ к охраняемой законом компьютерной информации, содержащейся на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло за собой уничтожение, блокировку, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети (ст. 272 УК РФ) [5].

5) Административная ответственность (за нарушение положений законодательства в области персональных данных, в том числе за нарушение правил распространения персональных данных)

Кодексом об административных правонарушениях предусмотрено несколько составов, которые могут быть применены в данном случае:

1. отказ в предоставлении информации (ст. 5.39 КоАП РФ) — т.е. неправомерный отказ в предоставлении гражданину и (или) организации информации, предоставление которой предусмотрено федеральными законами, несвоевременное ее предоставление либо предоставление заведомо недостоверной информации.

Ответственность, предусмотренная этой статьей КоАП РФ, может также наступить за несвоевременное предоставление запрошенной информации либо за предоставление заведомо недостоверной информации.

2. нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) (ст. 13.11 КоАП РФ);

3. разглашение информации с ограниченным доступом (ст. 13.14 КоАП РФ) — т.е. информации, доступ к которой ограничен федеральным законом (за исключением случаев, если разглашение такой информации влечет уголовную ответственность); др.

4. нарушение правил защиты информации (ст. 13.12 КоАП РФ)

5. за невыполнение предписания Роскомнадзора об устранении нарушений законодательства о персональных данных (ст. 19.5 КоАП РФ)

6. за оставление без ответа запроса этого органа касательно персональных данных (ст. 19.7 КоАП РФ);

7. за несоблюдение требований гл. 14 ТК РФ, регламентирующей вопросы защиты персональных данных работника, может наступить административная ответственность, предусмотренная ст. 5.27 КоАП РФ за нарушение трудового законодательства и иных нормативных правовых актов, содержащих нормы трудового права [3].

Если посмотреть судебную практику по вопросу исполнения законодательства о персональных данных, то можно отметить, что руководители организаций за неисполнение законодательства достаточно часто подвергаются административному наказанию в виде предупреждения или штрафа.

Санкция ст. 13.11 Кодекса Российской Федерации об административных правонарушениях за нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) влечет предупреждение или наложение административного штрафа на граждан в размере от 300 до 500 рублей; на должностных лиц - от 500 до 1000 рублей; на юридических лиц - от 5000 до 10 000 рублей.

Так, например, прокуратурой Юкаменского района была проведена проверка исполнения законодательства о персональных данных в ООО «Луч», который осуществлял сельскохозяйственную деятельность и деятельность по переработке древесины на территории Юкаменского района

Удмуртской Республики для своих личных нужд. Проведенной проверкой было установлено, что в ООО «Луч» Юкаменского района УР допускаются нарушения законодательства о персональных данных, а именно генеральным директором ООО «Луч» в нарушение вышеуказанного законодательства собираются, используются, хранятся, и передаются персональные данные 3 работников без их письменных согласий с момента их принятия на работу в целях контроля за их трудовой деятельностью, поощрения за труд и отчисления социальных платежей. Своими действиями генеральный директор ООО «Луч» совершила административное правонарушение, которое предусмотрено ст. 13.11 КоАП РФ - нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных).

Рассмотрим другой пример из судебной практики, где руководителем не разработан и не принят локальный нормативный акт, который регламентирует порядок хранения и использования персональных данных работников, не назначено лицо, ответственное за организацию обработки персональных данных, в связи с чем последний был привлечен к административной ответственности. Так, и. о. прокурора района имени Полины Осипенко Хабаровского края обратился в суд о привлечении к административной ответственности должностного лица - индивидуального предпринимателя Казакова В.А. (далее - ИП Казаков В.А.) за совершение административного правонарушения, предусмотренного ст. 13.11 Кодекса Российской Федерации об административных правонарушениях. В постановлении о возбуждении дела об административном правонарушении указано, что в ходе проведенной прокуратурой проверки соблюдения ИП Казаковым В.А. законодательства о защите прав и свобод человека и гражданина при обработке персональных данных выявлено, что Казаковым В.А. не разработан и не принят локальный нормативный акт, который регламентирует порядок хранения и использования персональных данных работников, не назначено лицо, ответственное за организацию обработки

персональных данных. Суд, рассмотрев материалы дела, постановил признать индивидуального предпринимателя Казакова виновным в совершении административного правонарушения, предусмотренного ст. 13.11 Кодекса Российской Федерации об административных правонарушениях (нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных)) и подвергнуть его административному наказанию в виде административного штрафа в размере 300 (трехсот) рублей.

При вынесении постановления суд ссылаясь на то, что в силу требований пунктов 1, 2 части 1 статьи 18.1, части 1 статьи 22.1 Федерального закона «О персональных данных» оператор обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных данным Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами, в том числе назначением оператором, являющимся юридическим лицом, ответственным за организацию обработки персональных данных; издание оператором, являющимся юридическим лицом, документов, определяющих политику оператора в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений.

При таких обстоятельствах суд счел вину должностного лица - ИП Казакова В.А. в совершении им административного правонарушения, предусмотренного ст. 13.11 КоАП РФ, установленной и доказанной.

Также участились случаи, когда руководитель организации привлекается к ответственности за правонарушение в связи с тем, что не было получено согласие работника на обработку персональных данных.

Согласно постановлению прокурора Унинского района Кировской области 22.03.2016 при проведении проверки соблюдения трудового

законодательства в деятельности МУП «Унинская МТС» выявлены нарушения действующего трудового законодательства, которые ущемляли основные права и интересы работников в сфере защиты персональных данных. В нарушение требований ст. 3, ст. 6, п. 1 ст. 9 Федерального закона от 27.07.2006 N 152-ФЗ «О персональных данных» согласие работников МУП «Унинская МТС» на обработку их персональных данных со всех работников не получено. Так, один из работников, принятый на работу 25.01.2016, на момент проверки 22.03.2016 не был ознакомлен с положением об организации работы с персональными данными под подпись.

Кроме того, не были установлены перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ; перечень мест хранения; перечень мер, необходимых для обеспечения сохранности персональных данных, порядок их принятия; перечень лиц, ответственных за реализацию указанных мер, в соответствии с требованиями п. 6, 13, 15 Постановления Правительства РФ от 15.09.2008 N 687. Лица, осуществляющие в силу своей трудовой деятельности обработку персональных данных (работники службы кадров, бухгалтерии), не были проинформированы об обработке ими персональных данных работников. Мировой судья судебного участка N 4 Унинского района Кировской области Осокин К.В., рассмотрев материалы дела, постановил признать директора МУП «Унинская МТС» виновным в совершении административного правонарушения, предусмотренного ст. 13.11 КоАП РФ, и назначить административное наказание в виде предупреждения.

Федеральный закон от 07.02.2017 № 13-ФЗ [8] расширил перечень оснований для привлечения работодателя к административной ответственности в области защиты персональных данных, а также увеличил размеры административных штрафов. Этот закон вступает в силу с 1 июля 2017 года. Административная ответственность в сфере персональных данных существенно ужесточена.

Новая редакция статьи 13.11 КоАП РФ содержит семь конкретных составов правонарушений и предусматривает соответствующие им штрафы с самым высоким из них – 75 тысяч рублей (для юридических лиц). В отличие от прошлой редакции ст.13.11, новая редакция статьи четко устанавливает случаи, за которые оператор персональных данных может понести наказание (Приложение А).

Таким образом, административные штрафы с 1 июля 2017 года существенно увеличатся, установленные новые размеры штрафов зависят от вида совершенного правонарушения. Привлекать к ответственности могут по разным составам правонарушений. Соответственно, за разные нарушения на одну компанию могут наложить несколько разных штрафов.

Частью 1 ст. 28.4 КоАП РФ предусмотрено, что до 1 июля 2017 года возбуждать дела по административным делам, связанным с персональными данными, по статье 13.11 КоАП РФ был вправе исключительно прокурор. С 1 июля 2017 года участие прокурора уже будет необязательным. Должностные лица Роскомнадзора с указанной даты дела по статье 13.11 КоАП будут вправе самостоятельно возбуждать. Такая поправка внесена комментируемым законом в пункт 58 части 2 статьи 28.3 КоАП РФ. Следовательно, процедура привлечения к ответственности по делам о персональных данных становится проще.

В части материальной, дисциплинарной, гражданско-правовой ответственности изменений с 01.07.2017 не планируется.

3. Локальное нормативно-правовое регулирование защиты персональных данных в трудовых правоотношениях

Обязанности оператора можно условно разделить на юридические (выражающиеся в совершении юридически значимых действий, принятии документов и т.д.) и на организационно-технические меры, которые имеют своей целью защиту персональных данных гражданина от разглашения.

К юридическим мерам относятся:

1. О получении согласия субъекта персональных данных в форме, обеспечивающей возможность доказать факт получения согласия (п.1 ст.9. Закона 152-ФЗ), либо в определенных законом случаях в письменной форме. Когда речь идет о передачи данных в страну, не обеспечивающей защиты персональных данных (подп.1п.4 ст.12 Закона №152-ФЗ), когда обрабатываются биометрические данные для целей установления личности (п.1 ст.11 Закона №152-ФЗ) или когда имеет место обработка специальных категорий персональных данных касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни (поп.1 п.2 ст.10 Закона №152-ФЗ). Согласно вступающей в силу ч.2. ст.13.11 КоАП РФ с 01.07.2017 неполучение письменного согласия является самостоятельным составом правонарушения, за которое предусмотрен штраф до 75 тыс.руб для юридических лиц.

2. Опубликование политики конфиденциальности или иного документа, определяющего его политику в отношении обработки персональных данных, и сведений о реализуемых требованиях к защите персональных данных, а также обеспечение возможности доступа к указанному документу с использованием средств соответствующей информационно-телекоммуникационной сети (п.2 ст.18.1 Закона №152-ФЗ). С 01.07.2017 нарушение такой обязанности повлечет штраф в размере 30 тыс.руб.

3. Издание локальных актов, устанавливающих процедуры,

направленные на предотвращение и выявление нарушений законодательства РФ, устранение последствий таких нарушений (подп.2 п.1 ст.18.1 Закона 152-ФЗ)

4. Направлять уведомление в Роскомнадзор об обработке персональных данных работников в случаях, предусмотренных законодательством РФ (ч.1 ст.22 Закона №152-ФЗ).

К организационно-техническим мерам относятся:

1. Обеспечение безопасности информационных систем и необходимого уровня защищенности персональных данных

2. Назначение лица ответственного за обработку персональных данных (ст.22.1 Закона №152-ФЗ)

3. Обеспечение невозможности несанкционированного доступа к материальному носителю биометрических персональных данных, а также иных требований, установленных Постановлением Правительства РФ от 06.07.2008 №512.

Устанавливать перечень лиц, осуществляющих обработку персональных данных, либо имеющих к ним доступ; перечень мест хранения; перечень мер, необходимых для обеспечения сохранности персональных данных, порядок их принятия; перечень лиц, ответственных за реализацию указанных мер, в соответствии с требованиями п. 6, 13, 15 Постановления Правительства РФ от 15.09.2008 N 687

Таким образом, обязательными документами для работодателя при работе с персональными данными являются:

1. Локальный нормативный акт (документ, определяющий политику оператора в отношении обработки персональных данных);

2. Уведомление о начале обработки персональных данных;

3. Письменная форма согласия на обработку персональных данных: для соискателя, для работника, для третьих лиц;

4. Приказ о назначении уполномоченного лица за организацию обработки персональных данных;

5. Инструкции по заполнению форм кадровых документов, в которых используются персональные данные;

6. Журнал учета (регистрации) движения документов, содержащие персональные данные работника.

В Трудовом кодексе РФ содержится требование документального закрепления и ознакомления работников с его правами в области защиты персональных данных, прописанное в п. 8 части первой ст. 86 Трудового кодекса РФ. В нем установлена необходимость обязательного ознакомления работников под расписку с документами организации, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области.

Чётких требований к структуре и содержанию данного локального акта действующее законодательство не содержит, но по общему смыслу он должен устанавливать порядок обработки персональных данных работников, их передачи, а также права, обязанности работника и работодателя, ответственность за нарушение установленных правил.

Локальный нормативный акт по персональным данным утверждается уполномоченным лицом в организации и не требует при утверждении учета мнения представительного органа работников.

Для обеспечения защиты персональных данных в организации и порядок их использования локальный нормативный акт, регламентирующий процедуру обработки персональных данных работника, должен содержать:

- круг вопросов, относящихся к персональным данным работников;
- перечень сведений, носящих конфиденциальный характер;
- круг лиц (перечень должностей), наделенных правом доступа к информации, составляющей персональные данные работников. (наличие перечня должностных лиц имеющих полный доступ, перечня должностных лиц имеющих ограниченный доступ (с указанием целей и перечня персональных данных));

- права и обязанности должностных лиц, осуществляющих обработку персональных данных работников;
- права работников на ознакомление со своими персональными данными, в том числе с участием своего представителя, на получение ими копий любой записи, содержащей их персональные данные, на полную информацию о своих персональных данных и обработке этих данных;
- порядок получения (сбора) персональных данных работников;
- порядок формирования информационных ресурсов;
- порядок хранения, использования и передачи третьей стороне работодателем персональных данных работников;
- порядок ознакомления работника, в том числе с участием своего представителя, со своими персональными данными;
- порядок получения работником копий любой записи, содержащей его персональные данные, полной информации о своих персональных данных и обработке этих данных ответственность должностных лиц за нарушение правил обработки персональных данных работников.

Рекомендации при разработке локального нормативного акта, регламентирующей обработку персональных данных:

1) в самом тексте документа необходимо указать, что это локальный нормативный акт. Это значит, что работодатель должен учитывать требования, установленные ст. 8 ТК РФ и не забывать, что нормы ЛНА не могут ухудшать положение работника по сравнению с нормами действующих законодательных и иных нормативных правовых актов.

2) Необходимо указать что работодатель обрабатывает не только персональные данные работников, но и соискателей, в случае если формирует так называемый внешний кадровый резерв, включающий резюме понравившихся соискателей, посетивших собеседование, но по каким-то причинам не ставшим работниками. Необходимо также указать, что работодатель продолжает осуществлять обработку (хранение) персональных

данных работников и после их увольнения в течении установленного архивного срока хранения

3) Обязательно ознакомить всех работников организации, включая временных, работающих по совместительству с документом регламентирующим обработку ПД под роспись.

4) В данный ЛНА включить в приложения согласие на обработку персональных данных, который необходимо грамотно сформулировать, текст которого должен зависеть от целей обработки ПД.

5) Уточнить перечень персональных данных, необходимых для данной организации. Так как трудоемкость защиты персональных данных напрямую зависит от степени важности обработки сведений

Разработанный проект положения «О защите персональных данных работников» (Приложение Б) устанавливает порядок получения, хранения, использования и защиты персональных данных работников в соответствии с Конституцией РФ, Трудовым кодексом РФ, Федеральным законом от 27 июля 2006 г. N 152-ФЗ «О персональных данных», Федеральным законом от 27 июля 2006 года N 149-ФЗ «Об информации, информационных технологиях и о защите информации».

Положение «О защите персональных данных работников» позволит выполнять работодателю необходимые требования действующего законодательства о персональных данных.

Положение «О защите персональных данных работников» разработано с целью установления единого порядка организации работы по обеспечению безопасности персональных данных при их обработке, закрепления механизма обеспечения прав и свобод работников на сохранение информации о фактах, событиях и обстоятельствах жизни работника, а также установления ответственности при выполнении операций с персональными данными работников.

Задачами настоящего Положения являются:

- регламентация порядка обработки персональных данных работников;

- обеспечение соблюдения законных прав и интересов организации и работников при обработке персональных данных;

- установления ответственности должностных лиц, имеющих доступ к персональным данным работников организации, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

Положение «О защите персональных данных работников» – локальный нормативный акт организации, регламентирующий, в соответствии с ТК РФ и иными федеральными законами, общие требования обработки персональных данных работников организации, обеспечение соответствия процедуры обработки персональных данных работников требованиям и нормам федеральных законов, локальных нормативных документов организации.

Положение распространяются на всех работников, обязательно для безусловного его исполнения и имеет целью обеспечить соблюдение законных прав и интересов организации и ее работников в связи с необходимостью получения, обработки, хранения и передачи сведений, составляющих персональные данные работников.

Таким образом, разработанный проект Положения внесет значимый результат в формировании политики в области персональных данных и позволит выполнять работодателю необходимые требования действующего законодательства о персональных данных.

В дальнейшем каждый поступающий на работу в организацию должен знакомиться с локальным актом, регламентирующим работу с персональными данными под подпись и предупреждаться об ответственности за его несоблюдение.

ЗАКЛЮЧЕНИЕ

Понимая важность и ценность информации о человеке, а также заботясь о соблюдении прав свобод граждан, государство требует от работодателей обеспечить надежную защиту персональных данных. Защита персональных данных – относительно новый институт, который является продолжением и конкретизацией конституционной нормы (ст. 23-24 Конституции РФ). Включение данного института в трудовое законодательство предоставляется весьма важным, т.к. это говорит о высоком уровне защиты работника от возможного вмешательства в его частную жизнь.

Обеспечение защиты информации и персональных данных является одним из приоритетных направлений и важнейшей задачей в обеспечении информационной безопасности любой организации. Но в связи с тем, что институт является относительно новым, существует множество нерешенных вопросов, которые зачастую препятствуют выполнению работодателям необходимых требований действующего законодательства о персональных данных.

В процессе написания работы выявлены следующие проблемы в области защиты персональных данных работников:

- главным законодательным источником о защите персональных данным является глава 14 ТК РФ «Защита персональных данных работника». При анализе данной главы выявляется несоответствие ее названия с содержанием, которое скорее включает в себя положения об обработке персональных данных, чем об их защите. В самой главе законодателем не дается определения защиты персональных данных работника, отсутствуют положения, включающие в себя конкретные действия, которые должен совершать работодатель для защиты персональных данных. В связи с этим порядок обработки, хранения персональных данных зачастую в каждой организации свой. Так как единый порядок не разработан на законодательном уровне.

- неточное определение субъекта, имеющего право на защиту персональных данных. ТК РФ защищает персональные данные работника, соискатель, бывший работник в качестве субъектов защиты не названы, что фактически ущемляет их права на защиту персональных данных. Отсутствует законодательное положение, определяющее включение либо невключение персональных данных работника сведений о родственниках, родителях, супруге, детях, хотя такие данные предоставляются при заполнении анкет.

- следующей проблемой, с которой сталкиваются работодатели – классифицирование сведений о работнике как персональных данных. В зарубежном опыте говорится о целесообразности разделения всей информации о работнике на две группы: данные общего характера и данные особого характера – персональные данные к которым относится информация о расовом происхождении, политических убеждениях, личных пристрастиях. Персональные данные второй группы должны иметь и особый режим защиты, больший уровень конфиденциальности. Понятие персональных данных данное законодателем настолько широко, что на практике часто возникают случаи является ли информация персональными данными или нет. (например, фотография работника, номер мобильного телефона).

Можно сделать вывод что, законодательство РФ о защите персональных данных нуждается в совершенствовании, необходима корректировка и уточнение некоторых имеющихся положений, которые в дальнейшем облегчат организацию работодателем защиты персональных данных.

Однако, есть и положительные моменты в совершенствовании законодательства. С 01 июля 2017 года в КоАП РФ внесены соответствующие изменения, благодаря которым в ст. 13.11 появятся новые составы административных правонарушений, а именно расширяется перечень оснований для привлечений к административной ответственности за незаконную обработку персональных данных.

Данное законодательное изменение является сигналом к тому, что государство стало внимательнее относиться к выполнению требований по защите персональных данных.

На сегодняшний момент, многие работодатели к защите персональных данных относятся легкомысленно, формально. Статья 13.11 КОАП РФ содержит всего один общий состав, предусматривающий одинаковую ответственность за любое нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах. Размер штрафа для юридических лиц может колебаться от 5000 до 10000 рублей. Данное наказание является малозначительным, давно не соответствует тяжести административного правонарушения и не обеспечивает превентивной функции, что в итоге как раз и приводит к массовому игнорированию требований действующего законодательства и нарушением в процессе их обработки.

Поэтому увеличение новой редакцией статьи 13.11 КоАП РФ максимального размера штрафа для юридических лиц до 75 000, изменит отношение многих работодателей к требованиям действующего законодательства в области работы с персональными данными. Учитывая последнюю практику проверяющих органов, когда за каждое выявленное в ходе одной проверки нарушение налагается отдельный штраф – общая сумма наказания может быть довольно существенной. В ходе исследования разобраны принятые изменения в области персональных данных по ужесточению административной ответственности с 01.07.2017г., рассмотрены новые составы административных правонарушений и увеличение штрафов.

Из проведенного анализа проблем регулирования персональных данных работника, можно сделать вывод, что работа с персональными данными работника – достаточно сложный процесс, который требует детального нормативно-правового регулирования. В связи с чем, законодатель устанавливает обязательность наличия локального

нормативного акта в каждой организации по работе с персональными данными. В ходе исследования разработаны предлагаемые рекомендации действий работодателя при формировании политики по защите персональных данных, которые детализированы в проекте положения «О защите персональных данных работников». Положение «О защите персональных данных» входит в перечень обязательных документов для работодателя при работе с персональными данными. Разработанный проект положения «О защите персональных данных работников» устанавливает порядок получения, хранения, использования и защиты персональных данных работников в соответствии с действующим законодательством. Он внесет значимый результат в формировании политики в области персональных данных и позволит выполнять работодателю необходимые требования действующего законодательства о персональных данных.

Таким образом, защита ПД – самостоятельный институт трудового права, регламентирующий обеспечение работнику его права на неприкосновенность информации, касающейся его профессиональной деятельности, а также некоторых аспектов его личной жизни, включающий понятие персональных данных работника и их обработки, общие требования при обработке персональных данных и гарантии их защиты, право работников в елях обеспечения защиты персональных данных, хранящихся у работодателя, вопросы ответственности за нарушение норм, регулирующих обработку и защиту персональных данных работника.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

Нормативные правовые акты

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) [Электронный ресурс]: с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 N 6-ФКЗ, от 30.12.2008 N 7-ФКЗ, от 05.02.2014 N 2-ФКЗ, от 21.07.2014 N 11-ФКЗ // Справочная правовая система «Консультант Плюс».- Режим доступа: <http://www.consultant.ru>

2. Гражданский кодекс Российской Федерации (часть первая) [Электронный ресурс]: федеральный закон от 30.11.1994 N 51-ФЗ ред. от 28.03.2017// Справочная правовая система «Консультант Плюс».- Режим доступа: <http://www.consultant.ru>

3. Кодекс Российской Федерации об административных правонарушениях [Электронный ресурс]: федеральный закон от 30.12.2001 N 195-ФЗ ред. от 07.06.2017 // Справочная правовая система «Консультант Плюс».- Режим доступа: <http://www.consultant.ru>

4. Трудовой кодекс Российской Федерации [Электронный ресурс]: федеральный закон от 30.12.2001 N 197-ФЗ ред. от 01.05.2017 // Справочная правовая система «Консультант Плюс».- Режим доступа: <http://www.consultant.ru>

5. Уголовный кодекс Российской Федерации [Электронный ресурс]: федеральный закон от 13.06.1996 N 63-ФЗ ред. от 07.06.2017 // Справочная правовая система «Консультант Плюс».- Режим доступа: <http://www.consultant.ru>

6. Об информации, информационных технологиях и о защите информации [Электронный ресурс]: федеральный закон Российской Федерации от 27 июля 2006 года N 149-ФЗ // Справочная правовая система «Консультант Плюс».- Режим доступа: <http://www.consultant.ru>

7. О персональных данных [Электронный ресурс]: федеральный закон от 27.07.2006 года № 152-ФЗ // Справочная правовая система «Консультант Плюс».- Режим доступа: <http://www.consultant.ru>

8. Об архивном деле в Российской Федерации [Электронный ресурс]: федеральный закон от 22 октября 2004 г. N 125-ФЗ // Справочная правовая система «Консультант Плюс».- Режим доступа: <http://www.consultant.ru>

9. О внесении изменений в Кодекс Российской Федерации об административных правонарушениях [Электронный ресурс]: федеральный закон от 07.02.2017 N 13-ФЗ // Справочная правовая система «Консультант Плюс».- Режим доступа: <http://www.consultant.ru>

10. Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации [Электронный ресурс]: постановление Правительства Российской Федерации от 15.09.2008 г. N 687 // Справочная правовая система «Консультант Плюс».- Режим доступа: <http://www.consultant.ru>

11. Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами [Электронный ресурс]: постановление Правительства РФ от 21.03.2012 N 211 // Справочная правовая система «Консультант Плюс».- Режим доступа: <http://www.consultant.ru>

12. Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных [Электронный ресурс]: постановление Правительства РФ от 01.11.2012 №1119 // Справочная правовая система «Консультант Плюс».- Режим доступа: <http://www.consultant.ru>

13. Об утверждении унифицированных форм первичной учетной документации по учету труда и его оплаты [Электронный ресурс]:

постановление Госкомстата России от 05.01.2004 №1// Справочная правовая система «Консультант Плюс».- Режим доступа: <http://www.consultant.ru>

14. Об утверждении административного регламента исполнения Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций государственной функции по осуществлению государственного контроля за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных [Электронный ресурс]: приказ Министерства связи и массовых коммуникаций Российской Федерации от 14.11.2011 г. N 312 // Справочная правовая система «Консультант Плюс».- Режим доступа: <http://www.consultant.ru>

15. Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных [Электронный ресурс]: приказ Федеральной Службы по техническому и экспортному контролю от 18 февраля 2013 г. N 21 // Справочная правовая система «Консультант Плюс».- Режим доступа: <http://www.consultant.ru>

16. Об утверждении требований и методов по обезличиванию персональных данных [Электронный ресурс]: приказ Роскомнадзора от 05.09.2013 N 996 // Справочная правовая система «Консультант Плюс».- Режим доступа: <http://www.consultant.ru>

Специальная литература

17. Абаев Ф.А. Историко-правовые предпосылки формирования и современные тенденции развития института персональных данных в трудовом праве // Пробелы в российском законодательстве. 2013. № 5. С. 136-139

18. Абаев Ф.А. Понятие, правовая природа персональных данных // Право и государство: теория и практика. 2014. № 3 (111). С. 126-131.

19. Аверченков В.И., Гайнулин Т.Р. Защита персональных данных в организациях/ В.И. Аверченков, Т.Р. Гайнулин. – Изд-во Флинта. – 2011, 124с.
20. Ануфриева Н.С. Правовые проблемы обработки персональных данных в трудовых отношениях // Актуальные проблемы современной юридической науки: Сборник научных трудов. Сургут: ИЦ СурГУ. 2012. С. 114-119
21. Астахова Л.В., Рублёв Е.Л. Проблемы защиты персональных данных в период смены нормативной базы и пути их решения // Вестник УрФО. Безопасность в информационной сфере. 2013. № 1 (7). С. 32-41
22. Беденкова А.А., Хоменко И.С. Правовой статус персональных данных работников // Вестник науки Сибири. 2014. № 4 (14). С. 148-151
23. Волкова О.Н. Персональные данные в трудовых отношениях: об истории вопроса // Образование. Наука. Научные кадры. 2014. № 5. С. 90-94
24. Гольпяпина И.Ю. О некоторых проблемах правового регулирования персональных данных работников // Юридическая наука и практика: история и современность: сборник материалов II Международной научно-практической конференции. 2014. № 2. С. 106-108
25. Гусов К.Н. Трудовое право: учебник для бакалавров / К.Н. Гусов.- М.: Изд-во Проспект, 2013 – 632 с.
26. Давыдова Е.В. Что работодателю необходимо знать о персональных данных // Кадровик. Кадровое делопроизводство. 2011. №4. С.10-15
27. Журавлев М.С. Персональные данные в трудовых отношениях: допустимые пределы вмешательства в частную жизнь работника // Информационное право. 2013. № 4. С. 35-38
28. Истратова А.Г. Актуальные вопросы защиты персональных данных работника // Юридические науки. 2014. №5. С. 14-18

29. Кутенков Ю.И. Понятие персональных данных работника в российском трудовом праве // Азиатско-тихоокеанский регион: Экономика, политика, право. 2015. № 4 (37). С. 116-133
30. Кутенкович Ю.И. Проблемы правового регулирования оборота персональных данных работников в трудовом законодательстве Российской Федерации // Экономико-правовые аспекты развития современного общества. 2013. С. 65-69
31. Кухаренко Т.А. Комментарий к Федеральному закону от 27.07.2006 №152-ФЗ «О персональных данных» (постатейный)» [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru>.
32. Лебедева М.М. Актуальные вопросы защиты персональных данных // Право: теория и практика. 2008. № 4 (105). С. 18-20
33. Лушников А., Лушникова М. Информация и персональные данные в сфере трудовых отношений // Кадровик. 2013. № 6. С. 19-24
34. Лушников А.М. Неприкосновенность частной жизни и персональные данные в сфере трудовых отношений: стратегия правотворчества в контексте мирового опыта // Юридическая техника. 2015. № 9. С. 410-417
35. Лютов Н.Л. Защита персональных данных: международные стандарты и внутреннее российское законодательство // Трудовое право. 2010. № 8 (126). - С. 15-32
36. Мазина Г.П. Персональные данные и их защита в трудовых и служебных правоотношениях // Общественная безопасность, законность и правопорядок в III тысячелетии. 2015. № 1-2. С. 180-185
37. Маркевич А.С. Теоретико-правовой анализ зарубежного законодательства о защите персональных данных в сфере трудовых отношений // Вопросы безопасности. 2016. № 3. С. 89-98

38. Маслеха М.А. Теоретические основы защиты персональных данных // Законность и правопорядок в современном обществе. 2012. № 8. С. 94-103
39. Меньшикова А.В. Некоторые проблемы защиты персональных данных работника, перспективы и пути их решения // Экономика и менеджмент инновационных технологий. 2014. № 11 (38). С. 156-159
40. Никольский В.А. Трудовое право РФ: учебно методический комплекс/ В.А. Никольский. – 2-е изд., допол и перераб. – М.: Изд. Центр ЕАОИ, 2011. - 412 с.
41. Организационно-правовая защита персональных данных в служебных и трудовых отношениях: Монография / Маркевич А.С.; под ред.: Занина Т.М. - Воронеж: Изд-во Воронеж. ин-та МВД России, 2009. - 114 с.
42. Петрыкина Н.И. Персональные данные личности: учеб. пособие/ Н.И. Петрыкина. – М.: МГИМО-Университет, 2012. – 98 с.
43. Петрыкина Н.И. Правовое регулирование оборота персональных данных. Теория и практика / Н.И. Петрыкина. – М.: Изд-во Статут, 2011. – 134 с.
44. Пилипенко С.Г., Федосин А.С. К вопросу о реализации права на защиту персональных данных при их обработке в электронной форме // Пробелы в российском законодательстве. 2009. № 3. С. 213-215
45. Саранчук Ю.М. Административная ответственность в области обработки персональных данных. // Закон и право. 2014. № 9. С. 143-146
46. Семинихин В.В. Кадровое делопроизводство/ В.В. Семинихин. – Изд-во ГроссМедиа, 2015. - 624 с.
47. Семинихин В.В. Ответственность организаций и их руководителей / В.В. Семинихин. – Изд-во ГроссМедиа, 2012.- 1040с.
48. Смоленский М.Б. Трудовое право РФ: учебник / М.Б. Смоленский. – Ростов-на-Дону: Феникс, 2011. – 491с.
49. Соколова Г.А. Персональные данные работников // Кадровая служба и управление персоналом предприятия. 2007. N 7. – С. 17-26

50. Станскова У.М. Состав персональных данных в трудовых отношениях: что подлежит защите // Кадровик. 2014. № 1. С. 16-23
51. Станскова У.М. Необеспечение конфиденциальности информации ограниченного доступа: проблемные аспекты дисциплинарной и материальной ответственности // Российский ежегодник трудового права. 2013. № 9. С. 319-329
52. Тифенцев Е.В. Некоторые проблемы защиты персональных данных работников // Защита трудовых прав: проблемы теории и практики: сборник научных статей. 2014. С. 85-100
53. Трудовое право России: учебник для бакалавров / отв. ред. Ю. П. Орловский. — М. : Издательство Юрайт, 2014. — 854 с.
54. Трудовое право России. Практикум: Учеб. пособ. / Отв. ред. И.К. Дмитриева, А. М. Куренной. — 2-е изд., перераб. и дополн. — М. : Юстицинформ; Издательский дом «Правоведение», 2011. — 792 с.
55. Челнокова Г.Б. Проблемы защиты персональных данных в рамках трудовых отношений // Право и государство: теория и практика. 2007. № 9. - С. 65-70

Судебная практика

56. Апелляционное определение Иркутского областного суда от 19.09.2013 по делу N 33-7662/2013
57. Определение Верховного суда Республики Саха (Якутия) от 23.10.2013 по делу N 33-4172/13
58. Постановление судебного участка №61 района имени Полины Осипенко Хабаровского края от 30.06.2016 по делу №5-79/2016
59. Постановление Унинского судебного района (Кировская область) от 05.04.2016 по делу №5-107/2016
60. Постановление Федерального арбитражного суда Северо-Западного округа от 13 мая 2009 г. по делу № А66-17/2009

ПРИЛОЖЕНИЕ А

Таблица 1 – Административная ответственность в соответствии с новой редакцией статьи 13.11 КоАП РФ

Состав административного правонарушения	Нарушаемая статья	Штраф для ДЛ	Штраф для ИП	Штраф для ЮЛ
Обработка персональных данных в случаях, не предусмотренных законодательством РФ , либо обработка персональных данных, несовместимая с целями сбора персональных данных, за исключением случаев, предусмотренных частью 2 настоящей статьи	Ст.5, ст.6 ФЗ №152	5 — 10 тысяч рублей	не предус мотрен	30 — 50 тысяч рублей
Обработка персональных данных без согласия в письменной форме субъекта персональных данных в случаях, когда такое согласие должно быть получено в соответствии с законодательством РФ, если эти действия не содержат уголовно наказуемого деяния, либо обработка персональных данных с нарушением установленных законодательством РФ требований к составу сведений, включаемых в согласие в письменной форме субъекта персональных данных на обработку его персональных данных	Ст.9 ФЗ №152	10 — 20 тысяч рублей	не предус мотрен	15 — 75 тысяч рублей
Невыполнение оператором предусмотренной законодательством РФ обязанности по опубликованию или обеспечению иным образом неограниченного доступа к документу, определяющему политику оператора в отношении обработки персональных данных, и сведениям о реализуемых требованиях к защите персональных данных	Ст.18.2 ФЗ №152	3 — 6 тысяч рублей	не предус мотрен	15 — 30 тысяч рублей
Невыполнение оператором предусмотренной законодательством РФ обязанности по предоставлению субъекту персональных данных информации, касающейся обработки его персональных данных	Ст.14, ст.20 ФЗ №152	4 — 6 тысяч рублей	10 — 15 тысяч рублей	20 — 40 тысяч рублей
Невыполнение оператором в сроки, установленные законодательством РФ, требования субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных об	Ст.21 ФЗ №152	4 — 10 тысяч рублей	10 — 20 тысяч рублей	25 — 45 тысяч рублей

<p>уточнении персональных данных, их блокировании или уничтожении в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки</p>				
<p>Невыполнение оператором при обработке персональных данных без использования средств автоматизации обязанности по соблюдению условий, обеспечивающих в соответствии с законодательством РФ сохранность персональных данных при хранении материальных носителей персональных данных и исключающих несанкционированный к ним доступ, если это повлекло неправомерный или случайный доступ к персональным данным, их уничтожение, изменение, блокирование, копирование, предоставление, распространение либо иные неправомерные действия в отношении персональных данных, при отсутствии признаков уголовно наказуемого деяния</p>	ПП №687	4 — 10 тысяч рублей	10 — 20 тысяч рублей	25 — 50 тысяч рублей
<p>Невыполнение оператором, являющимся государственным или муниципальным органом, предусмотренной законодательством РФ обязанности по обезличиванию персональных данных, либо несоблюдение установленных требований или методов по обезличиванию персональных данных</p>	ПП №211, приказ РКН №996	3 — 6 тысяч рублей	не предусмотрен	не предусмотрен

ПРИЛОЖЕНИЕ Б

ПОЛОЖЕНИЕ

УТВЕРЖДЕНО

«О защите персональных
данных работников»

приказом

от «___» _____ г.
№ _____

1 ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В целях настоящего Положения используются следующие основные термины и определения:

ПЕРСОНАЛЬНЫЕ ДАННЫЕ РАБОТНИКА (далее по тексту ПДР) - 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.

ОПЕРАТОР - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

ТРУДОВЫЕ ОТНОШЕНИЯ – отношения, основанные на соглашении между работником и работодателем о личном выполнении работником за плату трудовой функции (работы по должности в соответствии со штатным расписанием, профессии, специальности с указанием квалификации; конкретного вида поручаемой работнику работы), подчинении работника правилам внутреннего трудового распорядка при обеспечении работодателем условий труда, предусмотренных трудовым законодательством и иными нормативными правовыми актами, содержащими нормы трудового права, локальными нормативными актами, трудовым договором.

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

СУБЪЕКТ ПЕРСОНАЛЬНЫХ ДАННЫХ – физическое лицо, как носитель юридических прав и обязанностей.

ДОСТУП К ПДР – возможность получения персональных данных работников и их использования.

УПОЛНОМОЧЕННОЕ ЛИЦО – должностное лицо, назначаемое приказом организации, осуществляющее обработку ПДР.

АВТОМАТИЗИРОВАННАЯ ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ - обработка персональных данных с помощью средств вычислительной техники.

РАСПРОСТРАНЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ - действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

КОНФИДЕНЦИАЛЬНОСТЬ ИНФОРМАЦИИ - обязанность не раскрывать третьим лицам и не распространять персональные данные работника без его согласия, если иное не предусмотрено федеральным законом.

ПРЕДОСТАВЛЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

УНИЧТОЖЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

ОБЕЗЛИЧИВАНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

ИНФОРМАЦИОННАЯ СИСТЕМА ПЕРСОНАЛЬНЫХ ДАННЫХ - совокупность содержащейся в базе данных информации, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких сведений с использованием средств автоматизации или без использования таких средств.

2 ОБЩИЕ ПОЛОЖЕНИЯ

2.1 Положение «О защите персональных данных работников» (далее – Положение) – локальный нормативный акт организации, регламентирующий, в соответствии с ТК РФ и иными федеральными законами, общие требования обработки персональных данных работников организации, обеспечение соответствия процедуры обработки персональных данных работников требованиям и нормам федеральных законов, локальных нормативных документов организации.

2.2 Положение распространяется на всех работников, обязательно для безусловного его исполнения и имеет целью обеспечить соблюдение законных прав и интересов организации и ее работников в связи с необходимостью получения, обработки, хранения и передачи сведений, составляющих персональные данные работников.

2.3 Все вопросы, связанные с применением Положения, решаются Работодателем в пределах предоставленных ему прав, предусмотренных действующим законодательством и правилами внутреннего трудового распорядка.

3 СОСТАВ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1.1 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 свидетельстве о постановке на учет физического лица в налоговом органе на территории Российской Федерации;
- 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 о семейном положении, включая сведения о наличии иждивенцев;
- Фотография работника (биометрические данные);
- Информация о заработной плате;
- Биографические сведения;
- Сведения о наградах;
- Сведения о социальных льготах;
- Адрес места жительства и сведения о временном месте пребывания;
- Домашний и мобильный телефон;
- Алиментные обязательства, а также иные удержания из заработной платы, предусмотренные действующим законодательством;
- Сведения по страхованию работников, в том числе суммы страхования и размер страховых премий, перечисленных организацией в страховую организацию;
- Другая персональная информация.

3.1.2 В состав документов, содержащих персональные данные работников входят:

- Документы, сопровождающие процесс оформления трудовых отношений (паспорт, трудовая книжка, страховое свидетельство государственного пенсионного страхования; документы об образовании, о квалификации или наличии специальных знаний; документы воинского учета; личный листок по учету кадров; личная карточка работника Т-2);
- Штатная расстановка кадров;
- Личные дела работников;
- Учетные документы по личному составу, а также вспомогательные регистрационно-учетные формы, содержащие сведения персонального характера;
- Трудовые договоры с работниками, изменения и дополнения к трудовым договорам;
- Договоры о материальной ответственности работника, изменения и дополнения к ним;
- Организационно-распорядительные документы по личному составу (подлинники и копии);
- Списки работников;
- Электронные базы данных;
- Положения о структурных подразделениях;

- Должностные инструкции работников;
- Договор дополнительного медицинского страхования, изменения и дополнения к нему;
- Документы по оценке деловых и профессиональных качеств работников при приеме на работу;
- Документы, отражающие деятельность 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 справки, листки нетрудоспособности;
- Иные документы, содержащие сведения персонального характера.

4 ПОЛУЧЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1 Персональные данные работника следует получать у самого работника. Работник обязан предоставлять работодателю достоверную персональную информацию.

4.2 Информация, представляемая работником при поступлении на работу должна иметь документальную форму. При заключении трудового договора в соответствии со ст. 65 ТК РФ лицо, поступающее на работу, предъявляет:

- паспорт или иной документ, удостоверяющий личность;
- трудовую книжку, за исключением случаев, когда трудовой договор заключается впервые или работник поступает на работу на условиях совместительства или трудовая книжка у работника отсутствует в связи с ее утратой или по другим причинам;
- страховое свидетельство государственного пенсионного страхования;
- документы воинского учета - для военнообязанных и лиц, подлежащих воинскому учету;
- документ об образовании, о квалификации или наличии специальных знаний - при поступлении на работу, требующую специальных знаний или специальной подготовки;
- свидетельство о присвоении ИНН (при его наличии у работника);
- документы об обязательном предварительном медицинском осмотре (обследовании), обязательном психиатрическом освидетельствовании работников (при приеме на должности, требующие медицинского заключения о годности к их исполнению, а так же лицам, не достигшим возраста восемнадцати лет);
- документы о составе семьи (при желании работника) в целях предоставления ему возможных гарантий и компенсаций, для установленных законом условий труда с учетом семейного положения

4.3 При изменении персональных данных работник должен письменно уведомить об этом сотрудников отдела кадров в срок, не превышающий семи рабочих дней. Работодатель имеет право запрашивать у работника дополнительные сведения и документы, подтверждающие их достоверность.

4.4 В срок, не превышающий семи рабочих дней со дня предоставления работником или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, уполномоченное лицо обязано внести в них необходимые изменения.

4.5 Если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее (Приложение 1) и от него должно быть получено письменное согласие (Приложение 2). Уполномоченное лицо должно 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.

4.6 Уполномоченное лицо 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 статьей 24 Конституции Российской Федерации уполномоченное лицо вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия.

4.7 Уполномоченное лицо 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.

4.8 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.

5 ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ РАБОТНИКОВ

5.1 Доступ к ПДР разрешен только специально уполномоченным должностным лицам, которым персональные данные необходимы для выполнения конкретных трудовых функций. Список лиц, имеющих право доступа к персональным данным утверждается приказом в организации.

5.2 ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ РАБОТНИКОВ ВНУТРИ ОРГАНИЗАЦИИ (ВНУТРЕННИЙ ДОСТУП).

5.2.1 Правом полного доступа к информации, содержащей персональные данные работника, обладают:

- директор организации;
- заместители директора, главный бухгалтер, руководители структурных подразделений – к персональным данным работников, осуществляющих свои трудовые функции в подразделениях возглавляемых указанными лицами.
- начальник отдела кадров;
- работники в отношении своих персональных данных.

5.2.2 Лиц, допущенных к ПДР, знакомят под расписку с требованиями ТК РФ, иными федеральными законами, локальными нормативными актами организации (Приложение 3).

5.3 ДОСТУП ДРУГИХ ОРГАНИЗАЦИЙ И ГОСУДАРСТВЕННЫХ ОРГАНОВ К ПДР (ВНЕШНИЙ ДОСТУП).

5.3.1 Правом внешнего доступа к информации, содержащей персональные данные работника, обладают:

- инспекция труда, налоговая инспекция, пенсионный фонд, центры занятости населения, военкоматы, медицинские страховые компании, правоохранительные органы и другие организации в порядке, установленном Федеральными законами.

6 ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1 Обработка ПДР уполномоченным лицом возможна только с письменного согласия работника (Приложение 4).

6.2 Письменное согласие работника на обработку своих персональных данных должно включать в себя:

- фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- наименование предприятия, должность, фамилию и инициалы получающего согласие субъекта персональных данных;
- цель обработки персональных данных;
- перечень ПДР, на обработку которых дается согласие субъекта персональных данных;
- наименование предприятия, осуществляющего обработку персональных данных по поручению организации;
- перечень действий с ПДР, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;
- срок, в течение которого действует согласие, а также порядок его отзыва;
- подпись субъекта персональных данных.

6.3 В случае отзыва субъектом персональных данных согласия на обработку персональных данных (Приложение 5) уполномоченное лицо вправе продолжить обработку персональных данных без согласия субъекта в следующих случаях:

- ПДР являются общедоступными;
- обработка ПДР осуществляется в целях исполнения трудового договора;
- ПДР относятся к состоянию здоровья работника, и их обработка необходима для защиты его жизни, здоровья или иных жизненно важных интересов других лиц, и получение согласия работника невозможно;
- по требованию полномочных государственных органов в случаях, предусмотренных Федеральным законом;

- обработка ПДР осуществляется на основании ТК РФ или иного федерального закона, устанавливающего ее цель, условия получения ПДР и круг субъектов, ПДР которых подлежат обработке, а также определяющего полномочия работодателя;
- обработка ПДР осуществляется для статистических или иных научных целей при условии обязательного обезличивания ПДР.

6.4 В случае если работник отказывается предоставить письменное согласие на обработку персональных данных, составляется соответствующий акт (Приложение 6) с участием представителей работодателя в количестве не менее 3 человек, а обработка персональных данных работодателем осуществляется в соответствии со статьей 6 Федерального закона «О персональных данных».

6.5 В соответствии со ст. 86 ТК РФ в целях обеспечения прав и свобод человека и гражданина уполномоченные лица при обработке ПДР должны соблюдать следующие общие требования:

- обработка ПДР может осуществляться 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;
- при определении объема и содержания, обрабатываемых ПДР уполномоченное лицо должно руководствоваться Конституцией Российской Федерации, ТК РФ и иными федеральными законами;
- защита ПДР от неправомерного их использования или утраты обеспечивается работодателем за счет его средств в порядке, установленном ТК РФ или иными федеральными законами;
- работники и их представители должны быть ознакомлены под роспись с документами организации, устанавливающими порядок обработки ПДР, а также об их правах и обязанностях в этой области;

во всех случаях отказ работника от своих прав на сохранение в защиту тайны недействителен (ст. 86 ТК РФ).

7 ПЕРЕДАЧА, ЗАЩИТА И ХРАНЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1 При передаче персональных данных работников Работодатель обязан соблюдать следующие требования:

7.1.1 Не сообщать ПДР 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;

7.1.2 Не сообщать ПДР в коммерческих целях без его письменного согласия;

7.1.3 Предупредить лиц, получающих ПДР, 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;

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

7.1.5 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.

7.1.6 Персональные данные работников могут быть получены, проходить дальнейшую обработку и передаваться на хранение как на бумажных носителях, так и в электронном виде (посредством локальной компьютерной сети).

7.2 Уполномоченные лица при работе с ПДР обязаны:

7.2.1 Осуществлять внутренний контроль за соблюдением Работодателем и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;

7.2.2 Доводить до сведения работников Положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;

7.2.3 Организовывать прием и обработку обращений и запросов работников (заказ копий трудовых книжек, трудовых договоров, дополнительных соглашений к трудовому договору, справок: с места работы, на получение визы) и осуществлять контроль за приемом и обработкой таких обращений и запросов;

7.2.4 Изменения и дополнения в персональные данные вносить в дополнение к личному делу и (или) личную карточку Т-2 на основании документов, представленных работником. Устное заявление работника не является основанием для внесения изменений и дополнений в персональные данные.

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

7.4 Защита персональных данных работников от их неправомерного использования или утраты обеспечивается Работодателем за счет его средств и в порядке, установленном законодательством Российской Федерации.

7.5 Работники должны быть ознакомлены под роспись с документами Работодателя, устанавливающими порядок обработки персональных данных, а также об их правах и обязанностях в этой области.

7.6 При обработке и хранении документов, содержащих персональные данные, лица, получившие доступ к персональным данным работников организации, обязаны руководствоваться памяткой по организационным мерам защиты ПДР (Приложение 7).

8 ОБРАБОТКА ЗАПРОСОВ

8.1 ПЕРЕДАЧА ПЕРСОНАЛЬНЫХ ДАННЫХ ПО ЗАЯВЛЕНИЮ СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ

8.1.1 Прием и обработку обращений работников по запросам осуществляют сотрудники отдела кадров по письменному заявлению от работников (Приложение 8).

8.1.2 Работники имеют право на получение информации:

8.1.2.1 Касающейся обработки его персональных данных, в том числе:

- подтверждение факта обработки персональных данных оператором;
- правовые основания и цели обработки персональных данных;
- цели и применяемые оператором способы обработки персональных данных;
- сроки обработки персональных данных, в том числе сроки их хранения;
- иные сведения, предусмотренные статьей 14 Федерального закона «О персональных данных» или другими федеральными законами.

8.1.2.2 Копий документов, связанных с работой:

- копии приказа о приеме на работу, приказов о переводах на другую работу, приказа об увольнении с работы;
- копии трудовой книжки;
- справки: подтверждающую факт работы в организации, на получение визы и т.д.;
- иные сведения, предусмотренные ТК РФ.

8.1.2 Информацию, касающуюся обработки персональных данных работников работники отдела кадров обязаны предоставить в срок, не превышающий семи рабочих дней со дня поступления письменного заявления работника, информацию, связанную с работой не позднее трех рабочих дней со дня подачи заявления.

8.1.3 В случае отказа от предоставления запрашиваемой информации работники отдела кадров обязаны предоставлять письменный мотивированный отказ (Приложение 9). Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами, в том числе если:

- обработка персональных данных, включая персональные данные, полученные в результате оперативно-розыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;
- обработка персональных данных осуществляется органами, осуществившими задержание субъекта персональных данных по подозрению в совершении преступления, либо предъявившими субъекту персональных данных обвинение по уголовному делу, либо применившими к субъекту персональных данных меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством Российской Федерации случаев, если допускается ознакомление подозреваемого или обвиняемого с такими персональными данными;
- обработка персональных данных осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;
- доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц.

8.1.4 Гражданам (бывшим работникам), запрашивающим персональные данные о себе, указанные сведения предоставляются в соответствии с законодательством Российской Федерации. Порядок предоставления персональных данных осуществляется при строгом соблюдении требований по обеспечению защиты персональных данных от любых неправомерных действий в отношении таких данных.

8.2 ПЕРЕДАЧА ПЕРСОНАЛЬНЫХ ДАННЫХ В ПРЕДЕЛАХ ОРГАНИЗАЦИИ

8.2.1 Запросы на предоставление ПДР направляются на начальника отдела кадров по форме служебной записки, в котором обязательно указывается информация:

- о перечне ПДР или документов, содержащих ПДР, подлежащих передаче;
- о цели получения ПДР;
- о действиях с персональными данными;
- о необходимости заверки.

8.2.2 Запрос подлежит исполнению в течении 10 дней с даты поступления запроса на исполнение.

8.3 ПЕРЕДАЧА ПЕРСОНАЛЬНЫХ ДАННЫХ ТРЕТЬЕЙ СТОРОНЕ

8.3.1 Запрос от третьей стороны о передаче персональных данных работников подлежит исполнению при условии:

- передача осуществляется в соответствии с законодательством о государственной социальной помощи, трудовым законодательством, законодательством Российской Федерации о пенсиях по государственному пенсионному обеспечению, о трудовых пенсиях, об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-розыскной деятельности, об исполнительном производстве, уголовно-исполнительным законодательством Российской Федерации;
- передача персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

8.3.2 В иных случаях передача ПДР третьим лицам осуществляется при наличии письменного согласия на передачу персональных данных третьему лицу (Приложение 10).

8.3.3 При не соответствии запроса требованиям действующего законодательства или требованиям данного Положения, запрос исполнению не подлежит.

8.3.4 Уполномоченное лицо обязано вести учет документов, подготовленных к передаче, согласно запросов в Журнале учета (регистрации) движения документов, содержащих ПДР (Приложение 11).

9 ПРАВА И ОБЯЗАННОСТИ РАБОТНИКА В ОБЛАСТИ ОБРАБОТКИ И ЗАЩИТЫ ЕГО ПЕРСОНАЛЬНЫХ ДАННЫХ

9.1 РАБОТНИК ИМЕЕТ ПРАВО НА:

9.1.1 Полную информацию о своих персональных данных и обработке этих данных.

9.1.2 Свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные работника, за исключением случаев, предусмотренных федеральным законом.

9.1.3 Определение своих представителей для защиты своих персональных данных.

9.1.4 Доступ к своим медицинским данным с помощью медицинского специалиста по своему выбору.

9.1.5 Требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением законодательства Российской Федерации.

9.1.6 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.

9.1.7 Обжалование в суд любых неправомерных действий или бездействия работодателя при обработке и защите его персональных данных.

9.2 РАБОТНИК ОБЯЗАН:

9.2.1 При приеме на работу предоставлять работникам отдела кадров достоверные сведения о себе в порядке и объеме, предусмотренном действующим законодательством Российской Федерации.

9.2.2 В случае изменения сведений, содержащихся в документах, перечисленных в пункте 4.1.2 настоящего Положения, сообщать об этом работнику отдела кадров в течение семи рабочих дней с даты внесения изменений в соответствующие документы или с даты, когда работник узнал о внесении таких изменений.

10 ОТВЕТСТВЕННОСТЬ ДОЛЖНОСТНЫХ ЛИЦ РАБОТОДАТЕЛЯ ЗА НАРУШЕНИЕ НОРМ, РЕГУЛИРУЮЩИХ ОБРАБОТКУ И ЗАЩИТУ ПЕРСОНАЛЬНЫХ ДАННЫХ

10.1 Лица, виновные в нарушении требований закона "О персональных данных" несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством РФ ответственность.

11 ССЫЛКИ

В настоящем Положении использованы ссылки на следующие нормативные документы:

- Конституция Российской Федерации
- Трудовой кодекс Российской Федерации
- Кодекс Российской Федерации об административных правонарушениях
- Федеральный закон от 27.07.2006 г. № 152-ФЗ «О защите персональных данных»
- Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
- Постановление Правительства РФ от 17.11.2007 г. № 781 «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»

ПРИЛОЖЕНИЕ 1
ФОРМА УВЕДОМЛЕНИЯ О ПОЛУЧЕНИИ ПДР У ТРЕТЬЕЙ СТОРОНЫ

(должность, наименование подразделения)

(ФИО сотрудника **полностью**)

УВЕДОМЛЕНИЕ

от _____ № _____

*О получении персональных данных
у третьих лиц*

Уважаемый(ая),

Уведомляем Вас о том, что в соответствии с *Вашим заявлением об утрате трудовой книжки и просьбе оказать содействие в сборе сведений о предыдущих местах работы и периодах трудовой деятельности* (наименование организации) запросит эти персональные данные от третьих лиц. Данные сведения будут запрошены в целях *подтверждения страхового стажа*. Сведения будут запрашиваться в письменной форме при помощи *средств почтовой связи*. Просим Вас дать согласие на получение персональных данных от третьих лиц.

Начальник отдела кадров

(подпись)

(ФИО сотрудника)

С уведомлением ознакомлен(а),

(наименование должности)

(подпись)

(ФИО сотрудника)

« ____ » _____ 20__

ПРИЛОЖЕНИЕ 2

ФОРМА СОГЛАСИЯ НА ПОЛУЧЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ У ТРЕТЬЕЙ СТОРОНЫ

Директору

(ФИО)

(должность сотрудника **полностью**)

(ФИО сотрудника **полностью**)

(документ , удостоверяющий личность, кем когда выдан)

ЗАЯВЛЕНИЕ

*О согласии на получение
персональных данных у
третьей стороны*

Не возражаю против получения Вами сведений обо мне, содержащих *(данные о состоянии моего здоровья из поликлиники МУЗ «Городская больница» с целью решения вопроса о подборе мне работы, не противопоказанной по состоянию здоровья в документальной форме в течение двух месяцев)*.

Настоящее заявление может быть отозвано мной в письменной форме.

(подпись)

«___» _____ 20__

ПРИЛОЖЕНИЕ 3

ФОРМА РАСПИСКИ ОБ ОЗНАКОМЛЕНИИ С ТРЕБОВАНИЯМИ ТК РФ, ИНЫМИ ФЕДЕРАЛЬНЫМИ ЗАКОНАМИ, ЛОКАЛЬНЫМИ НОРМАТИВНЫМИ АКТАМИ

РАСПИСКА

Я, _____,
(Фамилия, Имя, Отчество)

имея доступ к персональным данным работников (наименование организации), настоящим уведомлен(а), что согласно статье 88 Трудового кодекса Российской Федерации (прилагается) и Федерального закона от 27.07.2006 г. № 152-ФЗ (в ред. от 25.07.2011) «О персональных данных», не имею права сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это требуется в целях предупреждения угрозы жизни и здоровья работника, а также в случаях, установленных Трудовым кодексом Российской Федерации или иными федеральными законами. С требованиями Положения «О защите персональных данных работников» ознакомлен(а).

До моего сведения доведены соответствующие положения по обеспечению сохранности персональных данных работников. Мне известно, что лица виновные в нарушении требований Трудового кодекса Российской Федерации, иных федеральных законов и локальных нормативных актов по получению, обработке распространению и использованию персональных данных работников несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

« _____ » 20 __ г.

Должность

подпись

Фамилия и инициалы

Статья 88. Передача персональных данных работника

При передаче персональных данных работника работодатель должен соблюдать следующие требования:

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 настоящим Кодексом РФ или иными федеральными законами;

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. Лица, получающие персональные данные работника, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется на обмен персональными данными работников в порядке, установленном настоящим Кодексом и иными федеральными законами;

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 работников представителям работников в порядке, установленном настоящим Кодексом или иными федеральными законами, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.

ПРИЛОЖЕНИЕ 4
ФОРМА СОГЛАСИЯ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ

Директору

(ФИО)

(должность сотрудника **полностью**)

(ФИО сотрудника **полностью**)

(документ , удостоверяющий личность, кем когда выдан)

ЗАЯВЛЕНИЕ

О согласии на обработку персональных данных

Я, _____,

в соответствии со статьей 9 Федерального Закона от 27.07.2006 №152-ФЗ (в ред. от 25.07.2011) «О персональных данных» не возражаю против получения Вами сведений обо мне, содержащих данные о фамилии, имени, отчестве, месте и дате рождения, адресе, семейном и социальном положении, образовании, доходах, профессии, состоянии здоровья, необходимых в связи с трудовыми отношениями, которые получены из представленных мной сведений в документальной форме с целью дальнейшего хранения, комбинирования, иного использования моих персональных данных в течение периода моей работы в (наименование организации)

Не возражаю против включения Вами сведений обо мне в общедоступные источники персональных данных (Справочники) на бумажных и электронных носителях, содержащих данные о фамилии, имени, отчестве, дате рождения, занимаемой должности (профессии), настоящем месте работы, табельном номере, служебном телефоне, фотографию, предполагаемом и фактическом времени проведения очередного отпуска с целью информационного обеспечения в (наименование организации) в течение периода моей работы в (наименование организации)

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

Разрешаю сотрудникам отдела кадров (наименование организации) производить обработку и передачу в пределах организации (на основании положения «О защите персональных данных») моих персональных данных (ФИО, паспортные данные, данные о трудовом стаже, данные об образовании). Разрешение дается мной на проведение сбора, анализа, статистической обработки данных в интересах обеспечения функционирования информационной системы персональных данных (наименование организации).

Я признаю за отделом кадров право прекратить мой доступ к Информационным ресурсам (наименование организации) после отзыва мной данного разрешения. В случае прекращения моего доступа к Информационным ресурсам по инициативе (наименование организации) данное разрешение считается немедленно отозванным.

Разрешение дается мной на период работы в наименование организации и может быть мной отозвано в любой момент по письменному заявлению.

« » _____ 201__ г.

**ПРИЛОЖЕНИЕ 5
ФОРМА ОТЗЫВА СОГЛАСИЯ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ
РАБОТНИКА**

Директору

_____ (ФИО)

_____ (должность сотрудника **полностью**)

_____ (ФИО сотрудника **полностью**)

_____ (документ , удостоверяющий личность, кем когда выдан)

ЗАЯВЛЕНИЕ

*Об отзыве согласия на обработку
персональных данных*

Я, _____
(фамилия, имя, отчество полностью)

В соответствии с п. 2 ст. 9 Федерального закона "О персональных данных" N 152-ФЗ от 27.07.2006 года отзываю у (наименование организации) согласие на обработку моих персональных данных.

Прошу прекратить обработку моих персональных данных в течение трех рабочих дней с момента поступления настоящего отзыва.

_____ (подпись)

« ____ » _____ 20__

ПРИЛОЖЕНИЕ 6
ФОРМА АКТА ОБ ОТКАЗЕ ПРЕДОСТАВЛЕНИЯ СОГЛАСИЯ НА ОБРАБОТКУ
ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКА

_____ (наименование предприятия)

АКТ

« » _____ 20 г.

_____ (время, дата составления акта, населенный пункт, место составления акта)

Об отказе от предоставления согласия
на обработку персональных данных

Мною, _____
(должность, Ф.И.О. работника, составившего документ)

в присутствии _____
(должность, Ф.И.О. работников, кроме составителя акта не менее 2 чел.)

составили настоящий акт о нижеследующем: _____
(дата, время, место составления акта)

работник _____
(должность, профессия, Ф.И.О.)

отказался от предоставления согласия на обработку его персональных данных

Содержание данного акта подтверждаем личными подписями:

_____ (должность)	_____ (подпись)	_____ (расшифровка подписи)
_____ (должность)	_____ (подпись)	_____ (расшифровка подписи)
_____ (должность)	_____ (подпись)	_____ (расшифровка подписи)

С актом ознакомлен:

_____ (должность, подразделение) _____ (подпись) _____ (расшифровка подписи)

Если ознакомление с актом невозможно в силу того, что работник отказывается от подписи в ознакомлении с актом заполнить часть 2

От подписи в ознакомлении с актом отказался

Содержание данного акта подтверждаем личными подписями:

_____ (должность)	_____ (подпись)	_____ (расшифровка подписи)
_____ (должность)	_____ (подпись)	_____ (расшифровка подписи)
_____ (должность)	_____ (подпись)	_____ (расшифровка подписи)

ПРИЛОЖЕНИЕ 7 ПАМЯТКА ПО ОРГАНИЗАЦИОННЫМ МЕТОДАМ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ

ПАМЯТКА

(по организационным мерам защиты
персональных данных работников)

Для защиты ПДР уполномоченные лица, а также лица, допущенные к ПДР при работе с персональными данными должны руководствоваться требованиями данной инструкции.

Защита персональных данных работника от неправомерного использования или утраты обеспечивается работодателем за счет его средств в порядке, установленном федеральным законом.

1 Для обеспечения внешней защиты ПДР приняты следующие меры:

1.1 Установлен пропускной режим и порядок приема, учета и контроля деятельности посетителей;

1.2 Используются технические средства охраны.

1.3 Помещения, в которых хранятся персональные данные работников, оборудуются надежными замками, системой видеонаблюдения, жалюзи, запираемыми шкафами, сейфами.

2 Для обеспечения внутренней защиты ПДР все сотрудники, работающие с персональными данными должны соблюдать следующие требования:

2.1 На рабочем столе лица, получившего доступ к персональным данным работников, должен находиться только определенный перечень документов, с которыми он в данный момент работает;

2.2 Документы, с которыми работа завершена, немедленно подшиваются в соответствующее дело или папку;

2.3 В случае работы на персональном компьютере, в котором содержатся персональные данные работников, работник не вправе допускать к нему других лиц, не имеющих право доступа к персональным данным, а также покидать рабочее место, в том числе и в течение рабочего дня, предварительно не выключив компьютер или не заблокировав его;

2.4 В конце рабочего дня все документы, содержащие персональные данные работников, должны быть убраны в запираемые шкафы или сейфы;

2.5 Запрещается:

- самостоятельно подключать к ПЭВМ какие-либо устройства и вносить изменения в состав, конфигурацию, размещение ПЭВМ;
- сообщать кому-либо устно или письменно личные атрибуты доступа к ресурсам ПЭВМ;

3 Хранение персональных данных работника в помещениях отдела учета и движения кадров осуществляется следующим образом

3.1 Трудовые книжки, печати и штампы хранить в несгораемом металлическом сейфе. Один экземпляр ключей от сейфа находится у работника, ответственного за работу с трудовыми книжками, второй экземпляр – у начальника отдела кадров

3.2 Личные дела, картотеки, учетные журналы и книги учета хранить в рабочее и нерабочее время в запираемом шкафу. Работникам отдела кадров не разрешается при выходе из помещения на время обеда или в конце рабочего дня оставлять какие-либо документы на рабочем столе или оставлять шкафы не запертыми.

3.3 Карточки в процессе работы с ними хранить в промежуточной рабочей картотеке, а после окончания работы – помещать в основные картотеки.

3.4 Уборка помещений отдела кадров допускается только в присутствии сотрудников отдела.

**ПРИЛОЖЕНИЕ 8
ФОРМА ЗАЯВЛЕНИЯ НА ПРЕДОСТАВЛЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ
РАБОТНИКОВ**

Директору

_____ (ФИО)

_____ (должность сотрудника **полностью**)

_____ (ФИО сотрудника **полностью**)

_____ (документ , удостоверяющий личность, кем когда выдан)

ЗАЯВЛЕНИЕ

На основании статьи 62 Трудового кодекса Российской Федерации и Федерального закона «О персональных данных» от 27.07.2006 г. № 152-ФЗ (в ред. от 25.07.2011) прошу выдать мне копии документов, связанных с работой:

- копия трудовой книжки _____ экз.;
- справка _____ ;
(указать о чем)
- копия приказа _____ ;
(указать о чем)
- иное _____

_____ .
(указать что)

_____ (подпись)

« _____ » _____ 20__

**ПРИЛОЖЕНИЕ 9
ФОРМА ОТКАЗА ОТ ПРЕДОСТАВЛЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ
РАБОТНИКОВ**

(уполномоченное лицо, направившее запрос либо)

(ФИО сотрудника **полностью**)

*Отказ от предоставления
персональных данных*

Уважаемый(ая),

На основании статьи 14 п. 8 Федерального закона от 27.07.2006 г. № 152-ФЗ в предоставлении запрашиваемой Вами информации отказано.

Начальник отдела кадров

(подпись, дата)

(ФИО)

**ПРИЛОЖЕНИЕ 10
ФОРМА СОГЛАСИЯ НА ПЕРЕДАЧУ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКА
ТРЕТЬИМ ЛИЦАМ**

Директору

(ФИО)

(должность сотрудника **полностью**)

(ФИО сотрудника **полностью**)

(документ, удостоверяющий личность, кем когда
выдан)

ЗАЯВЛЕНИЕ

*О согласии на передачу своих
персональных данных третьей стороне*

Не возражаю против передачи Вами сведений обо мне, содержащих персональные данные, а именно:

- копии трудовой книжки;
- справки с места работы с (без) указания заработной платы;
- должностной инструкции;
- сведений о работе для проведения медико-социальной экспертизы;
- копии диплома об образовании;

в МУЗ «Городская больница» в документальной форме в течение одного месяца.

Настоящее заявление может быть отозвано мной в письменной форме.

(подпись)

«____» _____ 20__

ПРИЛОЖЕНИЕ 11
ФОРМА ЖУРНАЛА УЧЕТА (РЕГИСТРАЦИИ) ДВИЖЕНИЯ ДОКУМЕНТОВ,
СОДЕРЖАЩИХ ПЕРСОНАЛЬНЫЕ ДАННЫЕ РАБОТНИКОВ

Журнал учета (регистрации) движения документов, содержащие ПДР

№ и дата входящего запроса	От кого (от куда) поступил запрос	Краткое содержание запроса	№ и дата исходящего ответа	Кому выдан документ по запросу	Кол-во	Исполнитель	Примечание

Красноярск 2017

Выпускник

Зыков
подпись, дата
05.06.2017

Т.Д. Ложникова
инициалы, фамилия

Руководитель

К.Ю.Н. Дюбен
подпись, дата
06.06.2017
должность, ученая степень

С.П. Басалаева
инициалы, фамилия

Тема

Защита персональных данных работника в России

код – наименование направления

40.03.01 - Юриспруденция

БАКАЛАВРСКАЯ РАБОТА

«*Юр*» 06
2017 г.

подпись

Е.И. Петрова

Заведующий кафедрой

УТВЕРЖДАЮ

Федеральное государственное автономное
образовательное учреждение
высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Юридический институт
Кафедра трудового и экологического права