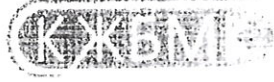
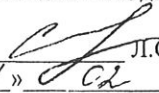


Введен в действие Приказом №П/40/1 от « 01 » 02 2018 г.



АКЦИОНЕРНОЕ ОБЩЕСТВО
«Красноярский комбинат железобетонных и
металлических конструкций»

УТВЕРЖДАЮ
Исполнительный директор


Л.С. Самохвалова
« 01 » 02 2018 г.

ПОЛОЖЕНИЕ № 3

О РАБОТЕ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ РАБОТНИКОВ
АО «КРАСНОЯРСКИЙ КОМБИНАТ ЖЕЛЕЗОБЕТОННЫХ И МЕТАЛЛИЧЕСКИХ
КОНСТРУКЦИЙ» И ИХ ЗАЩИТЕ

Красноярск
2018

Содержание

1 Цель.....	3
2 Общие положения	3
3 Нормативные ссылки	3
4 Термины и определения.....	3
5 Порядок работы	5
5.1 Понятие и состав персональных данных	5
5.2 Принципы обработки персональных данных.....	6
5.3 Согласие работника на обработку своих персональных данных	7
5.4 Организация хранения документов, содержащих персональные данные работников Общества	9
5.5 Уничтожение документов, содержащих персональные данные работников Общества.....	9
5.6 Доступ к персональным данным	10
5.7 Передача персональных данных.....	11
5.8 Защита персональных данных	13
5.8.1 Внутренняя защита	14
5.8.2 Внешняя защита	14
5.9 Ответственность за разглашение конфиденциальной информации, связанной с персональными данными.....	15
6 Лист согласования	16
7 Лист рассылки.....	17
Приложение 1 Обязательство о неразглашении персональных данных.....	18
Приложение 2 Форма заявления о согласии на обработку персональных данных	19
Приложение 3 Бланк запроса о предоставлении ПД (для третьих лиц)	22
Приложение 4 Бланк запроса о предоставлении ПД (для работников Общества)	23
Приложение 5 Форма Журнала учета выдачи/передачи ПД работников Общества.....	24

1 Цель

Целью настоящего Положения является развитие комплекса мер, направленных на обеспечение защиты персональных данных, хранящихся в АО «Красноярский комбинат железобетонных и металлических конструкций».

2 Общие положения

Настоящее Положение о работе с персональными данными работников Акционерного общества «Красноярский комбинат железобетонных и металлических конструкций» и их защите (далее Положение) устанавливает порядок приёма, учёта, сбора, поиска, обработки, накопления и хранения документов, содержащих сведения, отнесенные к персональным данным работников Акционерного общества «Красноярский комбинат железобетонных и металлических конструкций» (далее Общество).

Под работниками подразумеваются лица, имеющие трудовые отношения с Обществом.

Все работники Общества и их представители должны быть ознакомлены под подпись с настоящим Положением, а также другими документами Общества, устанавливающими порядок обработки персональных данных работников, а также их права и обязанности в данной области.

3 Нормативные ссылки

Основанием для разработки данного Положения являются:

- Конституция Российской Федерации;
- Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ;
- Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 г. № 195-ФЗ;
- Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ;
- Указ Президента Российской Федерации «Об утверждении перечня сведений конфиденциального характера» от 06.03.1997 № 188;
- Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ;
- Положение «Об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», утверждено Постановлением Правительства Российской Федерации от 17.11.2007 № 781.

Положение «Об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утверждено Постановлением Правительства Российской Федерации от 15.09.2008 № 687.

Положение и изменения к нему вводятся Приказом по общей деятельности и утверждаются Руководителем Общества.

4 Термины и определения

Блокирование персональных данных

Временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Информационная система персональных данных

Совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Использование персональных данных	Действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении работника либо иным образом затрагивающих его права и свободы.
Конфиденциальность персональных данных	Обязательное для соблюдения и исполнения требование к оператору и иному лицу, получившему доступ к персональным данным, не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом. Обязательным для соблюдения Обществом или иным, получившим доступ к персональным данным, лицом требование не допускать их распространение без согласия работника или наличия иного законного основания.
Обезличивание персональных данных	Действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.
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.
Общедоступные персональные данные	Персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия работника или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.
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.
Предоставление персональных данных	Действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.
Пароль	Секретная строка символов (букв, цифр, специальных символов), предъявляемая пользователем компьютерной системы для получения доступа к данным и программам; является средством защиты данных от несанкционированного доступа.

Пользователь (потребитель)	Работник Общества, использующий ресурсы информационной системы Общества для выполнения должностных обязанностей, а также юридические и физические лица, обращающиеся к Обществу или держателю персональных данных за получением необходимых сведений и пользующиеся ими без права передачи и разглашения.
Уничтожение персональных данных	Действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.
Учетная запись	Информация о сетевом пользователе: имя пользователя, его пароль, права доступа к ресурсам и привилегии при работе в системе, также может содержать дополнительную информацию (адрес электронной почты, телефон и т.п.).

5 Порядок работы

5.1 Понятие и состав персональных данных

Под персональными данными работников Общества понимается информация, необходимая Обществу в связи с трудовыми отношениями и касающаяся конкретного работника, а также сведения о фактах, событиях и обстоятельствах жизни работника, позволяющие идентифицировать его личность. Персональные данные всегда являются конфиденциальной, строго охраняемой информацией. К персональным данным относятся:

- дата и место рождения;
- гражданство;
- биографические сведения работника;
- сведения об образовании, специальности;
- занимаемая должность;
- стаж работы;
- идентификационный номер налогоплательщика (ИНН);
- страховой номер индивидуального лицевого счета (СНИЛС);
- сведения о воинском учете;
- льготы, на которые работник имеет право в соответствии с законодательством;
- адрес регистрации и фактического места жительства, домашний телефон;
- состав семьи, семейное положение;
- размер заработной платы;
- содержание трудового договора;
- состав декларируемых сведений о наличии материальных ценностей;
- содержание декларации, подаваемой в налоговую инспекцию;
- подлинники и копии приказов по личному составу;
- личные дела, личные карточки (форма Т-2), трудовые книжки работников;
- основания к приказам по личному составу;
- дела, содержащие материалы по повышению квалификации и переподготовке работников, их аттестации, служебным расследованиям;
- копии отчетов, направляемые в государственные органы;
- анкета (резюме);

– результаты медицинского обследования на предмет годности к осуществлению трудовых обязанностей (обработка данных сведений производится только в неавтоматизированном виде);

– фотографии и иные сведения, относящиеся к персональным данным работника.

Указанные документы являются конфиденциальными, но, учитывая их массовость и единое место обработки и хранения - соответствующий гриф ограничения на них не ставится.

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

Собственником информационных ресурсов (персональных данных) – является субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения этими ресурсами. Это любой гражданин, к личности которого относятся соответствующие персональные данные, и который вступил (стал работником) или изъявил желание вступить в трудовые отношения с Обществом. Субъект персональных данных самостоятельно решает вопрос передачи Обществу своих персональных данных.

Держателем персональных данных является Общество, которому работник добровольно передает во владение свои персональные данные. Общество выполняет функцию владения этими данными и обладает полномочиями распоряжения ими в пределах, установленных законодательством.

Права и обязанности Общества в трудовых отношениях осуществляются физическим лицом, уполномоченным руководителем Общества. Указанные права и обязанности он может делегировать нижестоящим руководителям – своим заместителям, руководителям структурных подразделений, работа которых требует знания персональных данных работников или связана с обработкой этих данных.

5.2 Принципы обработки персональных данных

Обработка персональных данных включает в себя их получение, хранение, комбинирование, передачу, а также актуализацию, блокирование, уничтожение.

Получение, хранение, комбинирование, передача или любое другое использование персональных данных работника может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении, обеспечения личной безопасности работника, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

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

Не допускается получение и обработка персональных данных работника о его политических, религиозных и иных убеждениях и частной жизни, а также о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных законодательством Российской Федерации (далее РФ).

При принятии решений, затрагивающих интересы работника, на основании его персональных данных не допускается использование данных работника, полученных исключительно в результате их автоматизированной обработки или электронного получения.

В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со ст. 24 Конституции РФ возможно получение и обработка данных о частной жизни работника только с его письменного согласия.

Пакет анкетно-биографических и характеризующих материалов (далее пакет) работника формируется после издания Приказа о его приеме на работу. Пакет обязательно содержит личную карточку формы Т-2, а также может содержать документы, содержащие персональные данные работника, в порядке, отражающем процесс приёма на работу.

Все документы хранятся в папках в алфавитном порядке фамилий работников.

Пакет пополняется на протяжении всей трудовой деятельности работника в данной организации. Изменения, вносимые в карточку Т-2, должны быть подтверждены соответствующими документами (например, копия свидетельства о браке).

Работник Отдела кадров, ответственный за документационное обеспечение кадровой деятельности, принимает от принимаемого на работу работника документы, проверяет полноту их заполнения и правильность указываемых сведений в соответствии с предъявленными документами.

Блокирование персональных данных происходит по требованию субъекта персональных данных при выявлении им недостоверности обрабатываемых сведений или неправомерных действий в отношении его данных.

При обработке персональных данных работников Общество в лице Исполнительного директора вправе определять способы обработки, документирования, хранения и защиты персональных данных работников на базе современных информационных технологий.

Работник обязан:

- передавать Обществу или его представителю комплекс достоверных, документированных персональных данных, состав которых установлен Трудовым кодексом РФ;
- своевременно, не позднее 10 рабочих дней с момента получения документов, сообщать Обществу об изменении своих персональных данных.

Работник имеет право на:

- полную информацию о своих персональных данных и обработке этих данных;
- свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные работника, за исключением случаев, предусмотренных законодательством РФ;
- определение своих представителей для защиты своих персональных данных;
- требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований законодательства РФ. При отказе Общества исключить или исправить персональные данные работника он имеет право заявить в письменной форме Обществу о своем несогласии с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера, работник имеет право дополнить заявлением, выражающим его собственную точку зрения;
- требование об извещении Обществом всех лиц, которым ранее были сообщены неверные или неполные персональные данные работника, обо всех произведенных в них исключениях, исправлениях или дополнениях;
- обжалование в суде любых неправомерных действий или бездействия Общества при обработке и защите его персональных данных.

5.3 Согласие работника на обработку своих персональных данных

Обработка персональных данных работников осуществляется Обществом только с их согласия либо без их согласия в следующих случаях:

- обработка персональных данных необходима для достижения целей, предусмотренных международным договором РФ или законом, для осуществления и

выполнения возложенных законодательством РФ на оператора функций, полномочий и обязанностей;

- обработка персональных данных необходима для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством РФ об исполнительном производстве (далее исполнение судебного акта);

- обработка персональных данных необходима для предоставления государственной или муниципальной услуги в соответствии с Федеральным законом от 27 июля 2010 года №210-ФЗ «Об организации предоставления государственных и муниципальных услуг», для обеспечения предоставления такой услуги, для регистрации субъекта персональных данных на едином портале государственных и муниципальных услуг;

- обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;

- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

- обработка персональных данных необходима для осуществления прав и законных интересов оператора или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

- обработка персональных данных необходима для осуществления профессиональной деятельности журналиста и (или) законной деятельности средства массовой информации либо научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и законные интересы субъекта персональных данных;

- обработка персональных данных осуществляется в статистических или иных исследовательских целях, за исключением целей, указанных в статье 15 Федерального закона №152-ФЗ, при условии обязательного обезличивания персональных данных;

- осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе (далее персональные данные, сделанные общедоступными субъектом персональных данных);

- осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с Федеральным законом «О персональных данных».

Согласие на обработку персональных данных может быть в любой момент отозвано работником.

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;

- фамилию, 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);

- наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта персональных данных;
- цель обработки персональных данных;
- перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка будет поручена такому лицу;
- перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;
- срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;
- подпись субъекта персональных данных.

5.4 Организация хранения документов, содержащих персональные данные работников Общества

Бумажные документы, содержащие персональные данные работников Общества, обязаны храниться в местах хранения, запирающихся на ключ, сейфах, металлических шкафах и т.п.

При работе с документами, содержащими персональные данные, запрещается:

- хранить документы в ящиках стола, оставлять без присмотра;
- брать документы для работы и на хранение домой;
- выносить документы из офиса без разрешения;
- держать документы вне сейфа без необходимости в процессе работы;
- передавать документы на хранение лицам, не имеющим права доступа к данным документам.

Текущее хранение кадровых документов, содержащих персональные данные работников, организует Отдел кадров Общества.

Правовое регулирование порядка и сроков хранения кадровых документов осуществляется на основе «Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения», утвержденного Приказом Минкультуры РФ от 25.08.2010 № 558.

Организация текущего хранения кадровых документов определяется Номенклатурой дел, утверждаемой Приказом Руководителя Общества.

Срок хранения информации в базах данных 1С соответствует сроку хранения аналогичных видов документов на бумажных носителях.

Подготовка документов к последующему хранению включает экспертизу практической ценности документов, оформление и описание дел, составление актов о выделении к уничтожению документов и передаче их в архив Общества.

5.5 Уничтожение документов, содержащих персональные данные работников Общества

Документы, содержащие персональные данные работников Общества, временного хранения, как правило, в архив Общества не передаются, а по истечении срока хранения уничтожаются.

К документам, содержащим персональные данные работников Общества, временного характера относятся документы, которые не должны храниться в архиве в обязательном порядке. Например: графики отпусков, графики медицинского обследования, заявления работников, справки по учебе, удостоверения работников, страховые полисы.

Для решения вопроса об уничтожении такого рода документов один раз в год собирается экспертная комиссия, состоящая из представителей Отдела кадров, Главного специалиста по стандартизации, Главного бухгалтера, Старшего юрисконсульта.

Итоги работы комиссии оформляются актами об уничтожении документов, содержащих персональные данные.

Уничтожение документов, содержащих персональные данные работников Общества, производится любым способом, исключающим ознакомление посторонних лиц с уничтожаемыми материалами и возможность восстановления их текста. Акты составляются и подшиваются в дело.

5.6 Доступ к персональным данным

Персональные данные добровольно передаются работником непосредственно держателю этих данных и потребителям внутри Общества исключительно для обработки и использования в работе.

Все работники Общества при приеме на работу обязаны подписывать Обязательство о неразглашении персональных данных работников Приложение 1.

Обязанность по исполнению требований по нераспространению сведений, содержащих персональные данные работников Общества, сохраняется за бывшими работниками Общества в течение всего срока действия конфиденциальности сведений.

Внешний доступ.

К числу потребителей персональных данных вне Общества относятся государственные и негосударственные организации:

- налоговые инспекции;
- правоохранительные органы;
- органы статистики;
- военкоматы;
- органы социального страхования;
- пенсионные фонды;
- государственные органы надзора и контроля;
- иные органы в соответствии с действующим Законодательством.

Внутренний доступ.

Внутри Общества к разряду потребителей персональных данных относятся работники Общества, которым эти данные необходимы для выполнения должностных обязанностей:

- Исполнительный директор;
- Главный инженер;
- Финансовый директор;
- Коммерческий директор;
- Директор по безопасности;
- Главный бухгалтер;
- Старший юрисконсульт;
- Специалисты Отдела кадров и ФЭО;
- сотрудники Бухгалтерии;
- Инженер информационных технологий;
- Системный администратор;
- Секретарь-референт;
- Руководители структурных подразделений (в отношении своих подчиненных);
- сотрудники Отдела охраны труда и окружающей среды (к персональным данным, содержащимся в листе прохождения обучения и проверке знаний требований охраны труда);

– сотрудники Медпункта (к персональным данным для прохождения медицинского осмотра).

Общество обязано обеспечивать безопасность персональных данных при их обработке, осуществлять защиту персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

Документы, содержащие персональные данные работников Общества, создаются:

- в виде записей в базах данных УПП 1С;
- в виде отдельных файлов (doc, xls и т.п.), создаваемых ответственными лицами.

Создание и хранение документов с персональными данными работников Общества в виде отдельных файлов (doc, xls и т.п.) допускается только на персональных компьютерах ответственных лиц.

Доступ работника к своим персональным данным.

По запросу работника Общество обязано не позднее 3-х рабочих дней со дня получения такого запроса выдать работнику копии документов на бумажном носителе, связанные с работой (копии Приказа о приеме на работу, Приказов о переводах на другую работу, Приказа об увольнении с работы, выписки из трудовой книжки, справки о заработной плате, периода работы у данного работодателя и др.).

Копии документов, связанных с работой, заверяются надлежащим образом и предоставляются работнику безвозмездно.

Общедоступные персональные данные

В категорию «общедоступные персональные данные» (в том числе для использования в телефонных справочниках, списках работников, базах данных и т.п.) с письменного согласия работников Приложении 2 включаются:

- Фамилия Имя Отчество;
- пол;
- должность;
- подразделение;
- номер паспорта, дата и место его выдачи;
- дата приема на работу, перевода (увольнения);
- номера служебных телефонов (внешних, внутренних, сотовых);
- адреса служебной электронной почты;
- адрес места работы, номер кабинета;
- дата рождения;
- стаж работы;
- сведения (даты) о нахождении в командировке, отпуске, на больничном;
- сведения об образовании, квалификации, курсах повышения квалификации;
- фотография;
- служебная характеристика и рекомендации.

По письменному требованию работника сведения о нем могут быть исключены из категории «общедоступные персональные данные».

5.7 Передача персональных данных

При передаче персональных данных работника Общество должно соблюдать следующие требования:

Передача внешнему потребителю:

– передача персональных данных от держателя или его представителей внешнему потребителю может допускаться в минимальных объемах и только в целях выполнения задач, соответствующих объективной причине сбора этих данных;

– при передаче персональных данных работника потребителям (в том числе и в коммерческих целях) за пределы АО «КЖБМК», Общество не должно сообщать эти данные третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника или в случаях, установленных федеральными законами;

– ответы на правомерные письменные запросы других фирм, учреждений и организаций даются с разрешения Руководителя Общества, либо лица, им уполномоченного, и только в письменной форме и в том объеме, который позволяет не разглашать излишний объем персональных сведений;

– не допускается отвечать на вопросы, связанные с передачей персональной информации по телефону или факсу;

– по возможности персональные данные обезличиваются;

– передача персональных данных работников контрольно-надзорным органам и в государственные информационные системы персональных данных (далее ИСПДн) осуществляется в соответствии с действующим Законодательством РФ.

– передача персональных данных работника для подготовки доверенностей и заказа билетов и гостиниц на период командировок осуществляется на основании согласия работника на предоставление персональных данных для доверенностей и заказа билетов, гостиниц Приложение 3;

– передача персональных данных для подготовки нотариальных доверенностей на работников Общества по предоставлению полномочий осуществляется на основании согласия на предоставление персональных данных нотариусу Приложение 3;

– передача персональных данных уполномоченным должностным лицам Банка для оформления и получения зарплатой банковской карты осуществляется на основании согласия на предоставление персональных данных Приложение 3;

– передача персональных данных работников благотворительным организациям, негосударственным пенсионным фондам, посольствам, другим организациям; родственникам, членам семьи и другим лицам осуществляется по письменному запросу о предоставлении персональных данных Приложение 3 на имя Руководителя Общества с указанием цели предоставления и характера персональных данных. Передача персональных данных осуществляется только при условии получения письменного согласия работника, данные которого запрашиваются (отметка о согласии должна быть проставлена работником на запросе), либо по письменному заявлению самого работника.

– все запросы о предоставлении персональных данных должны быть зарегистрированы в Журнале учёта выдачи/передачи персональных данных работников Общества Приложение 5.

Порядок рассылки третьим лицам документов, содержащих персональные данные работников Общества:

Процесс отправки третьим лицам документов конфиденциального характера, содержащих персональные данные работников Общества производится следующим образом:

– документы, содержащие персональные данные работников, передаются ответственным исполнителем уполномоченному работнику для последующей отправки адресату.

– данные по отправке (вид документа, дата документа, количество экземпляров, адресат, его почтовый адрес, ФИО ответственного исполнителя, дата отправки, вид отправки (заказным письмом, заказным письмом с уведомлением, экспресс-почтой и т.д.) собственноручно вносятся ответственным исполнителем в Журнал учета почтовых отправлений.

Отправка документов производится уполномоченным работником следующими способами - через отделение почтовой связи либо Службы по экспресс доставке почты и грузов.

Отправлять документы, содержащие персональные данные работников и/или информацию ограниченного распространения по электронной почте допускается только в крайнем случае с разрешения Директора по безопасности.

Отправка внешним адресатам электронной почты информации, содержащей конфиденциальную информацию, без криптографического преобразования (архивирования файла и его защиты паролем) **запрещена**.

Отправка внешним адресатам электронной почты информации, содержащей персональные данные, без криптографического преобразования с применением сертифицированных средств криптографической защиты информации **запрещена**.

Отправка документов на небумажных носителях производится в упаковке, соответствующей техническим требованиям сохранности носителей и записанной на них информации. Отправка электронных документов, записанных на машинные носители, производится при наличии сопроводительного письма.

Документы, поступающие к Секретарю для отправки, должны обрабатываться и отправляться по назначению не позднее следующего рабочего дня.

Передача внутреннему потребителю:

Общество вправе разрешать доступ к персональным данным работников.

Потребители персональных данных в письменной или электронной форме (по своему усмотрению) запрашивает у работника Отдела кадров необходимую ему информацию из личного дела работника, а также указывает, в каком виде информации должна быть предоставлена (в письменном виде, в виде пакета документов).

Если работник Отдела кадров не может предоставить сразу же запрашиваемую информацию, то согласовывается время и дата предоставления необходимой информации.

При оформлении запроса в письменном или электронном виде заполняется бланк «Запроса о предоставлении персональных данных (для работников Общества)» Приложение 4, где указываются, какие сведения о работнике необходимы. В соответствии со статьей 86 ТК РФ, персональные данные работника могут быть использованы в следующих случаях:

- в целях обеспечения соблюдения законов и иных нормативных правовых актов;
- в содействии работнику в трудоустройстве, обучении и повышении в должности;
- в обеспечение личной безопасности работников;
- при контроле количества и качества выполняемой работы и обеспечения сохранности имущества.

Работник Отдела кадров при получении запроса (в устной, письменной или электронной форме) регистрирует его в «Журнале учета выдачи / передачи персональных данных работников Общества» Приложение 5 и предоставляет информацию в требуемом виде и в установленные сроки.

5.8 Защита персональных данных

Под угрозой или опасностью утраты персональных данных понимается единичное или комплексное, реальное или потенциальное, активное или пассивное проявление злоумышленных возможностей внешних или внутренних источников угрозы создавать неблагоприятные события, оказывать дестабилизирующее воздействие на защищаемую информацию.

Риск угрозы любым информационным ресурсам создают стихийные бедствия, экстремальные ситуации, террористические действия, аварии технических средств и линий

связи, другие объективные обстоятельства, а также заинтересованные и незаинтересованные в возникновении угрозы лица.

Защита персональных данных представляет собой жестко регламентированный технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и, в конечном счете, обеспечивающий достаточно надежную безопасность информации в процессе управленческой и производственной деятельности Общества.

5.8.1 Внутренняя защита

Для защиты персональных данных работников необходимо соблюдать ряд мер:

- ограничение и регламентация состава работников, функциональные обязанности которых требуют знания персональных данных;
- строгое избирательное и обоснованное распределение документов и информации между работниками;
- рациональное размещение рабочих мест работников, при котором исключалось бы бесконтрольное использование персональных данных (защищаемой информации), обеспечение отдельными со звукоизоляцией кабинетами без прозрачных стен, обеспечение отдельными принтерами и сканерами.
- знание работниками требований нормативно – методических документов по защите информации и сохранении тайны;
- наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;
- определение и регламентация состава работников, имеющих право доступа (входа) в помещение, в котором находится вычислительная техника;
- организация порядка уничтожения информации;
- не допускается выдача личных дел работников на рабочие места руководителей. Личные дела могут выдаваться на рабочие места только Исполнительному директору, либо лицу им уполномоченному. Передача личных дел через Секретаря не допускается.
- персональные компьютеры, в которых содержатся персональные данные, должны быть защищены паролями доступа;
- персональные компьютеры, в которых содержатся персональные данные, должны быть защищены соответствующими средствами защиты информации;
- утверждается список лиц, имеющих право доступа и работы с электронными персональными данными работников.
- для каждого из ответственных лиц устанавливается индивидуальный логин и пароль доступа.

5.8.2 Внешняя защита

Для защиты персональных данных (конфиденциальной информации) создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лиц, пытающихся совершить несанкционированный доступ и овладение персональными данными (конфиденциальной информации).

Целью и результатом несанкционированного доступа к персональным данным (конфиденциальной информации) может быть не только овладение персональными данными и их использование, но и их видоизменение, уничтожение, внесение вируса, подмена, фальсификация содержания реквизитов документа и др.

Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности организации, посетители, работники других организационных структур.

Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих

материалов в подразделениях, имеющих право на внутренний доступ к персональным данным работников в силу своих функциональных обязанностей.

Для защиты персональных данных работников необходимо соблюдать ряд мер:

- соблюдать порядок приема, учета и контроля деятельности посетителей;
- осуществлять пропускной режим организации;
- осуществлять охрану территории, зданий, помещений, транспортных средств.

5.9 Ответственность за разглашение конфиденциальной информации, связанной с персональными данными

Персональная ответственность – одно из главных требований к организации функционирования системы защиты персональной информации и является обязательным условием обеспечения эффективности этой системы.

Руководитель, разрешающий доступ работника к конфиденциальному документу, несет персональную ответственность за данное разрешение.

Каждый работник Общества, получающий для работы конфиденциальный документ, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) влечет дисциплинарную, административную, гражданско-правовую или уголовную ответственность граждан и юридических лиц.

Ответственным за информационную безопасность в Обществе является Управляющий директор, который также является гарантом соблюдения Законодательства РФ персональных данных.

На Директора по безопасности возлагается:

- принятие мер по предотвращению разглашения и утечки сведений, содержащих персональные данные работников Общества;
- учет фактов утраты документов и разглашения сведений, содержащих персональные данные работников Общества, анализ причин и разработка мер по предупреждению таких инцидентов;
- обеспечение учета сейфов, металлических шкафов, специальных хранилищ и помещений (а также ключей к ним), в которых осуществляется хранение и работа с документами, содержащими персональные данные работников Общества;
- контроль за выполнением правил обращения с документами, содержащими персональные данные работников Общества.

На Начальника Отдела кадров возлагается:

- организация и ведение работы с информацией, содержащей персональные данные работников Общества;
- контроль за выполнением правил обращения с документами, содержащими персональные данные работников Общества;
- контроль за соблюдением установленного порядка копирования документов, содержащих персональные данные работников Общества, их учетом, хранением и использованием;
- контроль за соблюдением правил рассылки документов, содержащих персональные данные работников Общества.