Персональные данные

Жижерина Ю.Ю.
Бизнес-тренер, эксперт по трудовым отношениям

Нормативные акты

- Конституция Российской Федерации
- Федеральный закон от 19 декабря 2005 г. №160-ФЗ "О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных«
- Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации"
  Трудовой кодекс Российской Федерации от 30 декабря 2001 г. № 197-ФЗ
- Федеральный закон от 6 апреля 2011 г. № 63-ФЗ "Об электронной подписи"
- Федеральный закон от 7 мая 2013 г. №99-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием федерального закона "О ратификации Конвенции Совета Европы О защите физических лиц при автоматизированной обработке персональных данных«
- Федеральный закон от 27 июля 2006 г. №152-ФЗ "О персональных данных''

Персональные данные

Что относится к персональным данным:

любая информация, прямо или косвенно относящаяся к субъекту персональных данных (ст. 3 Закона о персональных данных), в частности:

- фамилия, имя, отчество
- пол, возраст
- изображение человека (фотография и видеозапись)
- образование, квалификация, профессиональная подготовка и сведения о повышении квалификации
- место жительства
- семейное положение, наличие детей, родственные связи
- факты биографии и предыдущая трудовая деятельность (место работы, судимость, служба в армии, работа на выборных должностях, на государственной службе и др.)
- финансовое положение
- деловые и иные личные качества, которые носят оценочный характер
- биометрические персональные данные
- специальные категории персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни
- иные сведения

К документам организации, содержащим персональные данные работников, относятся:

- анкета, автобиография, личный листок по учету кадров, которые заполняются работником при приеме на работу;
- копии документов, хранящиеся в личном деле работника: документа, удостоверяющего личность работника (паспорт), документов воинского учета, документа обязательного пенсионного страхования, свидетельств о заключении брака, рождении детей, документов об образовании;
- трудовая книжка;
- личная карточка по форме;
- трудовой договор и дополнительные соглашения к нему;
- подлинники и копии приказов по личному составу;
- документы оплаты труда;
- документы об обучении, оценке, аттестации работников;
- базы данных, обрабатываемые автоматически (например, таблицы Excel, базы программы 1С);
- при необходимости – иные документы, содержащие персональные данные работников.

Согласие на обработку персональных данных

Общее правило – обработка с согласия (ст. 6, 9 Закона о персональных данных)

Не требуется:

- в случаях, связанных с исполнением договора, в том числе трудового, но строго в целях трудоустройства и продвижения по службе

Требуется:

- дополнительная информация о работнике (номер его мобильного телефона, адрес личной электронной почты и т.д.)
- осуществление пропускного режима
- работа аутсорсинговой компании (кадровый, бухгалтерский учет)
- размещение в общедоступном источнике (сайт, стенд и т.д.)

Согласие на обработку должно содержать

- фамилию, имя, отчество, адрес, данные паспорта работника
- наименование или фамилию, имя, отчество и адрес работодателя
- цель обработки персональных данных
- перечень персональных данных, на обработку которых дается согласие
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению работодателя
- перечень действий с персональными данными, на совершение которых дается согласие, описание способов обработки персональных данных
- срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва
- подпись субъекта персональных данных

Получение персональных данных

- От работника
- из документов при приеме
- из анкеты
- по результатам обязательного медосмотра
- от кадрового агентства, действующего от имени соискателя
- из резюме соискателя, размещенного в сети Интернет и доступного неограниченному кругу лиц
- От третьих лиц (с согласия работника)

В согласии на получение:

- цели получения персональных данных работника у третьего лица
- предполагаемые источники информации (лица, у которых будут запрашиваться данные)
- способы получения данных, их характер
- возможные последствия отказа работодателю в получении персональных данных работника у третьего лица

Передача персональных данных

Общее правило - с согласия, в том числе в коммерческих целях

Не требуется:

- в целях предупреждения угрозы жизни и здоровью работника
- в налоговые органы, ФСС РФ, ПФР, в военные комиссариаты
- по запросу профсоюзов
- по запросу органов прокуратуры, ГИТ, суде, МВД, и т.д.
- в органы при несчастном случае

- А соискатели? - См. Разъяснения Роскомнадзора от 14.12.2012

Общее правило – от соискателей необходимо получать согласие

Исключение

•от имени соискателя действует кадровое агентство,

•самостоятельное размещение соискателем своего резюме в интернете,

Если резюме получено по каналам электронной почты, факсимильной связи, то работодателю необходимо получить согласие соискателя на их передачу и использование. Также согласие получают, если кандидат принес резюме лично.

Когда кандидат оставляет свои данные на сайте организации, у него должна быть возможность ознакомиться с политикой на сайте

Что необходимо сделать работодателю:

1. **Оформить локальный нормативный акт** (Положение/Политика о защите персональных данных) (ст. 87 ТК РФ) и ознакомить работников

Рекомендации по составлению документа, определяющего политику оператора в отношении обработки персональных данных, Роскомнадзор http://www.rkn.gov.ru/personal-data/p908/

в Политику рекомендуется включить :

- Общие положения
- Цели сбора персональных данных
- Объем и категории обрабатываемых персональных данных
- Порядок и условия обработки персональных данных
- Актуализация, исправление, удаление и уничтожение персональных данных
- Ответственность

Портал Роскомнадзора о персональных данных https://pd.rkn.gov.ru/

2. Назначить ответственное лицо приказом (ст. 22.1 Закона о персональных данных), закрепить в должностной инструкциии

3. Закрепить лиц, имеющих доступ к пересыльным данным (кадровики, бухгалтера, непосредственные руководители) приказом

4. Получить обязательство о нераспространении от лиц, имеющих доступ, дополнить долж. инструкции

5. Получать согласие об обработке/передаче/получении

6. Организовывать хранения (ст. ст. 86-87):

Защита данных (издать приказ при необходимости):

- сейфы
- металлические запираемые шкафы
- деревянные запираемые шкафы
- специально оборудованные помещения
- программная защита (Постановлением Правительства РФ от 01.11.2012 N 1119)

Роструд ! по соблюдению обязательных требований за 2 квартал 2017 года: хранить в личных делах с согласия

7. Если на сайте, то:

Согласие на обработку с отметкой

Доступ к политике (положении)

8**. Техническая часть** – Модель угроз (Приказ ФСТЭК России от 18.02.2013 N 21, Постановление Правительства РФ от 01.11.2012 № 1119)

9. Уведомлять Роскомнадзор?

https://pd.rkn.gov.ru/operators-registry/operators-list/ - реестр операторов

Не требуется при обработке ПДн, если они:

- относятся к субъектам, которых связывают с оператором трудовые отношения (Постановление от 11.01.2018 по делу № 57/5-21/2018).;
- получены оператором при заключении договора, но не распространяются, не предоставляются третьим лицам без согласия на то их субъекта, то есть используются оператором исключительно для исполнения договора;
- являются общедоступными ПДн;
- включают только ФИО субъектов ПДн;
- нужны для однократного пропуска субъекта ПДн на территорию, на которой находится оператор, или в иных аналогичных целях;
- включены в федеральные автоматизированные информационные системы ПДн, государственные информационные системы ПДн, созданные в целях защиты безопасности государства и общественного порядка;
- обрабатываются без использования средств автоматизации в соответствии с федеральными законами или иными нормативными правовыми актами.
- **Статья 13.23 КоАП -** непредставление документов – до 20 тыс. руб.

Ответственность за нарушение защиты персональных данных

ФЗ от 07.02.2017 N 13-ФЗ "О внесении изменений в КоАП РФ» - ужесточение ответственности с 01.07.2017

Было: любые нарушения (ст.13.11 КоАП)– до 10 тыс.

Стало (ст.13.11 КоАП):

- обработка персональных данных в «иных» целях – до 50 тыс.
- обработка персональных данных без согласия – до 75 тыс.
- нет доступа к политике по обработке данных – до 30 тыс.
- сокрытие информации об обработке – до 40 тыс.
- невыполнение требований об уточнении или блокировке – 45 тыс.
- необеспечение сохранности – 50 тыс.
- возбуждать дела вправе Роскомнадзор без прокурора (п. 58 ч. 2 ст. 28.3 КоАП РФ)

Ответственность работника, работающего с персональными данными

Административная ответственность (ст. 13.14 КоАП РФ): разглашение информации с ограниченным доступом лицом, получившим доступ в связи с исполнением профессиональных обязанностей, штраф: на граждан - от 500 до 1000 руб.; на должностных лиц - от 4000 до 5000 руб.

Дисциплинарная ответственность: выговор, увольнение (пп. "в" п. 6 ч. 1 ст. 81 ТК РФ)

Материальная ответственность (п. 7 ч. 1 ст. 243 ТК РФ)

Гражданско-правовая ответственность: моральный вред (ст. ст. 151, 1099

Уголовная ответственность (ст. 137 УК РФ): незаконное собирание или распространение сведений о частной жизни лица без его согласия либо распространение этих сведений в публичном выступлении лишение свобода до 2 лет, с использованием служебного положения до 4 лет

Проверки Роскомндзора

- https://rkn.gov.ru/plan-and-reports/ план проверок

Роскомнадзор:

- проверяет сведения, указанные организацией в Уведомлении;
- может требовать от оператора уничтожения недостоверных или полученных незаконным путем персональных данных;
- может ограничивать доступ к информации, обрабатываемой с нарушением законодательства;
- вправе обращаться в суд с исковыми заявлениями в защиту прав субъектов персональных данных и представлять их в суде;
- наделен полномочиями по привлечению к административной ответственности лиц, виновных в нарушении настоящего Федерального закона;
- обязан рассматривать жалобы и обращения по вопросам, связанным с обработкой персональных данных, а также принимать по ним решения в пределах своих полномочий.

Проверки Роскомндзора

- Плановые, Внеплановые
- Документарные ,выездные

Проверка - 20 дней. Итог проверки- акт.

Отрасли: образование, медицина, туризм, финансовые услуги и управляющие компании.

38%— государственные организации, коммерческие -62% мероприятий. Практически

99,8% — это юридические лица, а не индивидуальные предприниматели.

Примерные перечень документов:

- Уведомление об обработке ПДн
- Документ, определяющий ответственного за организацию обработки ПДн
- Перечень сотрудников, допущенных к обработке ПДн
- Документ, определяющие места хранения ПДн
- Справка об обработке специальных и биометрических категорий ПДн
- Справка об осуществлении трансграничной передачи ПДн
- Типовые формы документов с ПДн
- Порядок уничтожения ПДн
- Порядок передачи ПДн третьим лицам
- Типовая форма согласия на обработку ПДн
- Порядок учета обращений субъектов ПДн
- Перечень информационных систем персональных данных (ИСПДн), Документы, регламентирующие резервирование данных в ИСПДн, Перечень используемых средств защиты информации
- Матрица доступа, Модель угроз, Документ, определяющий уровни защищенности, Журнал учета машинных носителей ПДн

Статистика

По результатам 65% плановых проверок – есть нарушения

1 место (11% случаев - представление в уполномоченный орган уведомления об обработке персональных данных, содержащего неполные и (или) недостоверные сведения.

2 место (9%) — непринятие оператором мер, необходимых и достаточных для обеспечения выполнения обязанностей,

3 место (7%) разделили: а) несоответствие типовых форм документов, требованиям законодательства Российской Федерации; б) непредставление в уполномоченный орган сведений о прекращении обработки персональных данных или об изменении информации, содержащейся в уведомлении об обработке персональных данных.

4 место (по 6%)

- Несоблюдение оператором требований по информированию лиц, осуществляющих обработку
- Обработка персональных данных в случаях, не предусмотренных законом
- Отсутствие у оператора места (мест) хранения персональных данных (материальных носителей), перечня лиц, осуществляющих обработку персональных данных, либо имеющих к ним доступ.
- Несоответствие содержания письменного согласия субъекта персональных данных на обработку персональных данных требованиям законодательства Российской Федерации.