

СОВЕЩАНИЕ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В УПРАВЛЕНИИ ОБРАЗОВАНИЯ БРЯНСКОГО РАЙОНА

«17» октября 2016года

С 2006 года в России ведется усиленная работа над защитой персональных данных.

В течение этого времени был принят закон «О персональных данных», внесены поправки в Трудовой кодекс РФ, подписан приказ «О методах и способах защиты информации», которым должен следовать каждый, кто участвует в процессе получения, обработки и хранения персональных данных.

Теперь на работодателя ложится большая ответственность за защиту данных о сотруднике. Пострадать за небрежное отношение к персональным данным может и вся организация, и отдельный сотрудник отдела кадров, например. Но и рядовые сотрудники должны держать ухо востро, знать, как положено защищать информацию о них, и что вообще считать «личным».

Что относится к персональным данным?

На самом деле, почти все, что позволяет вас идентифицировать, – это персональные данные: ФИО, дата и место рождения, место жительства, семейное положение, образование, профессия, зарплата и др. Список законодатель оставил открытым.

Какие законы защищают персональные данные?

Основной документ в этом вопросе – Федеральный закон «О персональных данных» (№ 152-ФЗ). Согласно ему, любой государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, обязаны защитить их.

С 1 июля 2011 года все отношения, связанные с обработкой и хранением персональных данных, должны быть приведены в соответствие с требованиями настоящего Федерального закона.

В Трудовом кодексе РФ защите персональных данных сотрудника со стороны работодателя посвящена глава 14.

«Защита персональных данных в трудовых отношениях представляет собой регламентированный технологический процесс, предупреждающий нарушение установленного порядка доступности, целостности, достоверности и конфиденциальности персональных данных. Работодателем должны быть приняты следующие меры:

- пропускной режим,
- особый порядок приема, учета и контроля деятельности посетителей,
- использование технические средств охраны,

- лицензированное ПО, которое, как предполагается, защищает от его кражи злоумышленниками. Однако, с другой стороны, использование лицензированного ПО (а это, как правило, Windows), теоретически позволяет трансграничный съем любых данных с компьютеров. Поэтому, подписывая согласие на обработку персональных данных, важно указывать цели такой обработки, получить информацию о держателе базы (куда можно отправить отзыв согласия на обработку), и запрет на трансграничную передачу данных.

С июля 2009 года в закон были внесены поправки, отменившие обязанность операторов шифровать данные при их передаче или обработке. То есть, если отдельным законом эта обязанность не налагается, то работодателя не могут обязать обеспечить активную защиту. Но пассивную защиту ваших данных путем удаленного доступа к ним работодатель обеспечить обязан».

Что нужно защищать работодателю?

- Личную информацию о сотрудниках.
- Внутреннюю документацию организации.
- Информацию о контрагентах.

От кого защищать? Есть три источника угрозы: третьи лица; сотрудники, имеющие доступ к персональным данным; сам сотрудник.

Как защищать?

Согласно главе 14 ТК РФ, внутри организации должен действовать локальный нормативный акт, регулирующий порядок использования и хранения персональных данных. С этим актом должны быть ознакомлены все сотрудники. Кроме того, каждый принимаемый на работу кандидат должен знать об условиях обработки его персональных данных еще до заключения трудового договора (статья 68 ТК РФ).

Работодатель по закону берет на себя обеспечение технической защиты. Должны быть сейфы с кодами доступа или шкафы, запирающиеся на замок, для персональных данных, обрабатываемых без автоматизации. Доступ к ним должен быть только у сотрудников, допущенных к работе с персональными данными.

Важно, чтобы прием сторонних посетителей и прием сотрудников осуществлялся в отделе кадров в разное время. На столе работника, ведущего прием, не должно быть никаких документов, кроме тех, которые касаются конкретного посетителя.

Персональные данные, которые обрабатываются в информационных системах, также должны быть защищены. Методы защиты перечислены в приказе ФСТЭК РФ от 5

февраля 2010 г. № 58 «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных». Среди них:

- реализация разрешительной системы допуска пользователей (обслуживающего персонала) к информационным ресурсам, информационной системе и связанным с ее использованием работам, документам;
- учет и хранение съемных носителей информации и их обращение, исключаящее хищение, подмену и уничтожение;
- резервирование технических средств, дублирование массивов и носителей информации;
- использование защищенных каналов связи;
- предотвращение внедрения в информационные системы вредоносных программ (программ-вирусов) и программных закладок.

«Понять сотруднику, что меры безопасности по сохранности персональных данных предпринимаются в компании, можно по наличию (и ознакомлению под подпись) положения о защите персональных данных, приказа о доступе к персональным данным, наличию сейфа для кадровой документации, паролей на компьютерах.

Опасность для сотрудника заключается в том, что с лицензионного ПО можно получить персональные данные на конкретного сотрудника, сформировать любое досье на него, зарплатах, связях, родственниках, переписке. И в дальнейшем, так как все-таки идея тотальной электронизации овладела миром, при получении виз, оформлении загранпаспортов, в случае определенного интереса органов опеки к вашей семье, можно получить информацию о вас, ваших обязанностях, доходе, т.е. тех сведениях, которые можно использовать против вас».

Наказания

За несоблюдение положений закона 152-ФЗ «О персональных данных» предусмотрены гражданская, уголовная, административная, дисциплинарная и другие виды ответственности. В некоторых случаях может быть приостановлена деятельность организации или отзыв лицензии.

Трудовой кодекс предусматривает в качестве одного из оснований увольнения разглашение персональных данных другого работника (статья 81).

Но уволить за разглашение персональных данных можно только того работника, которому такие сведения стали известны в связи с исполнением трудовых обязанностей. Среди этих сотрудников: работники отдела кадров, бухгалтерии, руководители организаций и их заместители. Важный момент: для увольнения работника за разглашение персональных данных не важно, был ли проступок совершен умышленно или по неосторожности.

[illegible]

[illegible]