Негосударственное образовательное учреждение дополнительного профессионального образования «Учебный центр «Системэнерго»

Утверждаю:
Директор негосударственного образовательного учреждения дополнительного профессионального образования "Учебный центр "Системэнерго"
_____ Козлов Б.И.
"19" октября 2010г.

Положение о защите персональных данных руководителей и специалистов предприятий, проходящих обучение и предаттестационную подготовку в учебном центре «Системэнерго»

Общие положения

Настоящее Положение устанавливает порядок приема, учета, обработки и хранения документов, содержащих сведения, отнесенные к персональным данным руководителей и специалистов предприятий, проходящих обучение и предаттестационную подготовку в учебном центре «Системэнерго».

Настоящее Положение разработано на основании следующих документов:

- Федерального закона от 27.07.2006г. №152-ФЗ «О персональных данных»;
- Трудового кодекса РФ;

Настоящее Положение является развитием комплекса мер, направленных на обеспечение защиты персональных данных, используемых при оформлении документов в процессе обучения.

Оформление документов в процессе обучения регламентируется следующими документами:

- Федеральным законом от 21.07.1997г. №116-ФЗ «О промышленной безопасности опасных производственных объектов» с изм.
- Приказом Федеральной службы по экологическому, технологическому и атомному надзору от 29 января 2007г. №37 «О порядке подготовки и аттестации работников организаций, поднадзорных Федеральной службе по экологическому, технологическому и атомному надзору» с изм.
- Постановлением от 13 января 2003г. Министерства труда и социального развития Российской Федерации №1, Министерства образования Российской Федерации №29 «Об утверждении порядка обучения по охране труда и проверки знаний требований охраны труда работников организаций»

Положение о защите персональных данных и изменения к нему вводятся приказом, все сотрудники должны быть ознакомлены с данным Положением под расписку.

1. Понятие и состав персональных данных

Под персональными данными сотрудников понимается информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного сотрудника, а также сведения о фактах, событиях и обстоятельствах жизни сотрудника, позволяющие идентифицировать его личность.

Персональные данные всегда являются конфиденциальной, строго охраняемой информацией.

Учебным центром для оформления документов используются следующие персональные данные:

- Фамилия, Имя, Отчество;
- год, месяц, дата рождения;
- паспортные данные;
- образование;
- место работы
- специальность;
- занимаемая должность;
- адрес местожительства;
- домашний телефон

Документы, указанные в настоящем Положении, являются конфиденциальными, хотя, учитывая их массовость и единое место обработки и хранения – соответствующий гриф ограничения на них не ставится.

2. Обработка персональных данных

Под обработкой персональных данных понимается получение, хранение, комбинирование, передача или любое другое использование персональных данных работника.
При определении объема и содержания обрабатываемых персональных данных руководителей и специалистов предприятий, проходящих обучение и предаттестационную подготовку в учебном центре «Системэнерго», персонал учебного центра руководствуется Конституцией Российской Федерации, Трудовым кодексом и иными федеральными законами и постановлениями указанными в разделе 1 настоящего положения.
Обработка персональных данных производится в целях оформления необходимой документации в ходе учебного процесса и аттестации.
Получение персональных данных может осуществляться как путем представления их самим работником, так и путем получения их от организации заказчика.
Организация заказчик, на основании договора на обучение, заключенного с учебным центром, предоставляет списки слушателей для прохождения обучения. Информация содержит фамилию, имя, отчество и сведения о месте работы, занимаемой должности.
В процессе обучения слушатель заполняет анкету. Анкета содержит следующие данные:
Фамилия, Имя, Отчество; год, месяц, дата рождения; образование; место работы; специальность, занимаемая должность; адрес местожительства; домашний телефон.
Заполняя анкету, слушатель дает письменное согласие на обработку его персональных данных.
Полученные персональные данные используются исключительно для ведения учебного процесса и оформления документов при аттестации.
К обработке, передаче и хранению персональных данных слушателя могут иметь доступ:
- методисты учебного центра
- заведующая учебной части
- заместитель директора по учебно-методической работе

Все меры конфиденциальности при сборе, обработке и хранении персональных данных слушателя распространяются как на бумажные, так и на электронные носители информации. Не допускается отвечать на вопросы, связанные с передачей персональной информации по телефону или факсу.
Хранение персональных данных должно происходить в порядке, исключающем их утрату или их неправомерное использование. Для этих целей на операционных системах установлены логины, пароли; ограничен доступ в помещения, где хранятся персональные данные.

3. Доступ к персональным данным

Право доступа к персональным данным слушателей имеют:
- директор учебного центра и его заместитель
- заведующая учебной части
- методисты учебного центра

Перечень лиц, имеющих доступ к персональным данным слушателей, определяется приказом директора организации.
Надзорно-контрольные органы имеют доступ к информации только в сфере своей компитенции.

4. 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 и динамически-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 предприятия.
Защита персональных данных работника от неправомерного их использования или утраты должна быть обеспечена работодателем за счет его средств в порядке, установленном федеральными законами.
Внутренняя защита.
Основным виновником несанкционированного доступа к персональным данным является, как правило, персонал, работающий с документами и базами данных. Регламентация доступа персонала к конфиденциальным сведениям, документам и базам данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий между руководителями и специалистами организации.
Для обеспечении внутренней защиты персональных данных работников необходимо соблюдать ряд мер:
- ограничение и регламентация состава работников, функциональные обязанности которых требуют конфиденциальных знаний;
- строгое избирательное и обоснованное распределение документов и информации между работниками;
- знание работником требований нормативно-методических документов по защите информации и сохранении тайны;
- определение и регламентация состава работников, имеющих право доступа (входа) в помещение, в котором находится вычислительная техника;
- организация порядка уничтожения информации;
- своевременное выявление нарушения требований разрешительной системы доступа работниками подразделения;
- воспитательная и разъяснительная работа с сотрудниками подразделения по предупреждению утраты ценных сведений при работе с конфиденциальными документами;
Защита персональных данных сотрудника на электронных носителях обеспечена паролями.
Внешняя защита
Для защиты конфиденциальной информации создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лица, пытающегося совершить несанкционированный доступ и овладение информацией. Целью и результатом несанкционированного доступа к информационным ресурсам может быть не только овладение ценными сведениями 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 компании, 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 отделе персонала.
Для обеспечения внешней защиты персональных данных сотрудников необходимо соблюдать ряд мер:
- порядок приема, учета и контроля деятельности посетителей;
- пропускной режим организации;
- учет и порядок выдачи удостоверений;
- технические средства охраны, сигнализации;
- порядок охраны территории, зданий, помещений, транспортных средств;
- требования к защите информации при интервьюировании и собеседованиях.
Все лица, связанные с получением, обработкой и защитой персональных данных, обязаны подписать обязательство о неразглашении персональных данных работников.

5. Ответственность за разглашение конфиденциальной информации, связанной с персональными данными

Персональная ответственность - одно из главных требований к организации функционирования системы защиты персональной информации и обязательное условие обеспечения эффективности этой системы.

достоверности и конфиденциальности персональных данных и, в конечном счете обеспечивающий достаточно надежную безопасность информации в процессе управленческой и производственной деятельности предприятия.
Защита персональных данных работника от неправомерного их использования или утраты должна быть обеспечена работодателем за счет его средств в порядке, установленном федеральными законами.
Внутренняя защита.
Основным виновником несанкционированного доступа к персональным данным является, как правило, персонал, работающий с документами и базами данных. Регламентация доступа персонала к конфиденциальным сведениям, документам и базам данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий между руководителями и специалистами организации.
Для обеспечении внутренней защиты персональных данных работников необходимо соблюдать ряд мер:
- ограничение и регламентация состава работников, функциональные обязанности которых требуют конфиденциальных знаний;
- строгое избирательное и обоснованное распределение документов и информации между работниками;
- знание работником требований нормативно-методических документов по защите информации и сохранении тайны;
- определение и регламентация состава работников, имеющих право доступа (входа) в помещение, в котором находится вычислительная техника;
- организация порядка уничтожения информации;
- своевременное выявление нарушения требований разрешительной системы доступа работниками подразделения;
- воспитательная и разъяснительная работа с сотрудниками подразделения по предупреждению утраты ценных сведений при работе с конфиденциальными документами;
Защита персональных данных сотрудника на электронных носителях обеспечена паролями.
Внешняя защита
Для защиты конфиденциальной информации создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лица, пытающегося совершить несанкционированный доступ и овладение информацией. Целью и результатом несанкционированного доступа к информационным ресурсам может быть не только овладение ценными сведениями 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 компании, 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 отделе персонала.
Для обеспечения внешней защиты персональных данных сотрудников необходимо соблюдать ряд мер:
- порядок приема, учета и контроля деятельности посетителей;
- пропускной режим организации;
- учет и порядок выдачи удостоверений;
- технические средства охраны, сигнализации;
- порядок охраны территории, зданий, помещений, транспортных средств;
- требования к защите информации при интервьюировании и собеседованиях.
Все лица, связанные с получением, обработкой и защитой персональных данных, обязаны подписать обязательство о неразглашении персональных данных работников.

5. Ответственность за разглашение конфиденциальной информации, связанной с персональными данными

Персональная ответственность - одно из главных требований к организации функционирования системы защиты персональной информации и обязательное условие обеспечения эффективности этой системы.