Обработка персональных данных в ТулГУ

Супонин Александр Викторович
Начальник отдела информационной безопасности

ТулГУ, 2021

Что относится к персональным данным (п.1 ст 3 закона №152-ФЗ)

Персональные данные — любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных)

Имя (фамилия, имя, отчество) и документы, подтверждающие личность
Пол, возраст и анатомические характеристики (рост, вес и др.), биометрические данные (изображение на фотографии)
Сведения об образовании, квалификации, прохождении стажировки,
наличии разряда и др.
Сведения о состоянии здоровья
Место жительства
Национальная, этническая и расовая принадлежность
Сведения об увлечениях и привычках, в том числе вредных. Особенности взаимоотношений и общения с другими людьми (семейное положение и др.)
Религиозные и политические убеждения! (принадлежность к конфессий, Членство в политической партии, участие в общественных объединениях и др.)
Финансовое положение (доходы, долги, владение недвижимым имуществом, денежные вклады и др.)
Сведения о деловых и иных личностных качествах, которые носят оценочный характер.

Нормативная база обработки персональных данных

1. Конституция РФ
2.Трудовой Кодекса РФ 30.12.2001 №197-ФЗ (ред. от 03.07.2016 №348-ФЗ)
3. ФЗ Российской Федерации «О персональных данных» №152-ФЗ от 27.07.2006 » (в ред. от 22.02.2017 №16-ФЗ)
4. № 519-ФЗ «О внесении изменений в Федеральный закон 152-ФЗ»
5. Указ Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении Перечня сведений конфиденциального характера»
6. Постановление правительства: от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»
7. Внутренние нормативные документы ТулГУ:
   «Политика в отношении персональных данных»
   «Правила обработки персональных данных»
   «Положение о защите информации»
 - эти документы выложены на сайте университета, ссылка http://tsu.tula.ru/docs/oib.

Конфиденциальный характер персональных данных

1. Персональные данные относятся к категории конфиденциальной информации, которые указаны в Перечне сведений конфиденциального характера (утвержден Указом Президента РФ от 6 марта 1997 г. Ns 188 «Об утверждении Перечня сведений конфиденциального характера»), работодатель, получающий доступ к персональным данным, должен обеспечить конфиденциальность таких данных.
2. Постановлением Правительства РФ от 17 ноября 2007 г. № 781 утверждено Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных установлены требования к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, представляющих собой совокупность персональных данных, содержащихся в базах данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации.
3. Постановлением Правительства РФ от 15 сентября 2008 г. № 687 утверждено Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации.

Распространения персональных данных

С 1 марта 2021 года убирается понятие «общедоступные персональные данные». Утверждена норма - любую личную информацию о субъекте можно размещать только с его прямого согласия.

Получателями персональных данных работника па законном основании являются:

1. Органы социального страхования, органы пенсионного обеспечения; налоговые органы;
2. Органы прокуратуры и другие правоохранительные органы федеральная
3. Инспекция груда
4. Профессиональные союзы
5. Другие органы и организации в случаях, предусмотренных федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»

Законодательные акты по работе с персональными данными с использованием средств вычислительной техники **запрещают:**

1. Использовать компоненты программного и аппаратного обеспечения ПК в неслужебных целях; самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ПК
2. Осуществлять обработку конфиденциальной информации совместно с посторонними (не допущенными к данной информации) лицами
3. Записывать и хранить конфиденциальную информацию на неучтенных носителях информации (USB флешнакопителях; CD, DVD магнитных дисках и т. п.)
4. Оставлять включенными без присмотра свои ПК, не активировав средства защиты от несанкционированного доступа (временную блокировку экрана и клавиатуры)
5, Оставлять без личного присмотра на рабочем месте или где бы то ни было машинные носители и распечатки, содержащие конфиденциальную информацию
6. Предпринимать попытки несанкционированного доступа к недоступным информационным ресурсам, осуществлять намеренное изменение, уничтожение, чтение, или передачу информации неавторизованным способом.

Несколько правил по работе с персональными данными

1. С 1 марта 2021 года работодатели не вправе распространять персональные данные о сотруднике без его согласия (п. 1 ст. 10.1 Федерального закона от 27.07.2006 № 152-ФЗ в ред. от 30.12.2020). Этот означает, что размещать где-либо сведения о человеке без его согласия нельзя — ни на корпоративном сайте, ни на какой-либо страничке в соцсети — нигде.

2. Запрашивать только те данные, которые нужны для каждой конкретной цели. Например, нельзя запрашивать паспортные данные или домашний адрес для осуществления рассылки по электронной почте, использовать данные только для тех целей, о которых вы предупредили человека;

3. Перед получением персональных данных, которые предполагается публиковать в общедоступных источниках, получать письменное согласие на их обработку, хранение и распространение;

4. Персональные данные на бумажных носителях должны находиться в недоступном для посторонних лиц месте, в шкафах или ящиках столов, оборудованных замками, запирающимися на ключ;

5. Помещения, в которых ведется обработка персональных данных, запираются на ключ, а в нерабочее время дополнительно опечатываются. Ключи от помещений ежедневно сдаются на вахту здания.

Обеспечить безопасность чужих персональных данных просто

Чужие персональный данные нужно хранить так же, как вы храните конфиденциальную информацию о себе, при этом надо помнить, что при работе с персональными данными запрещается:

1. Передавать персональные данные по телефону
2. Оставлять без присмотра документы, оставлять в помещении посторонних лиц без присмотра и оставлять в свое отсутствие незапертым помещение, в котором осуществляется обработка персональных данных
3. Передавать ключи, от мест хранения и обработки персональных данных посторонним лицам; передавать личные атрибуты доступа (логин, пароль) к информационным системам персональных данных и базам данных
4. Использовать чужие атрибуты доступа (логин, пароль) для обработки персональных данных; использовать при обработке персональных данных личный ноутбук, личный USB-флешнакопитель и т.д
5. Выносить документы и другие носители информации, содержащие персональные данные за пределы ТулГУ
6. Использовать в качестве черновиков документы, содержащие персональные данные

Новые штрафы с 2017 года в области персональных данных

Система государственного надзора и контроля в области персональных данных

- Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор)
- Федеральная служба по техническому и экспортному контролю (ФСТЭК)
- Федеральная служба безопасности (ФСБ)
- Федеральная инспекция труда

В соответствии с приказом №1868 от 29.12.2017 ответственными за обработку персональных данных являются руководители институтов, управления и отделов. Ответственным за информационную безопасность являются начальник отдела информационной безопасности.

Обработка ПД в случаях, не предусмотренных законодательством, повлечет за собой следующие штрафы:

- 2000 - 6 000 рублей для граждан;
- 10 000 - 20 000 для должностных лиц;
- 60 тыс. - 100 тыс. для юрлиц.

Также вводится норма об ужесточении наказания, если нарушение повторится:

- 4 000 - 12 000 рублей для граждан;
- 20 000 - 50 000 для должностных лиц;
- 50 тыс. -100 тыс. для предпринимателей;
- 100 тыс. - 300 тыс. для юрлиц.

При возникновении угрозы несанкционированного доступа к персональным данным или попыткам хищения носителей, содержащих персональные данные работникам ТулГУ, необходимо незамедлительно сообщить в ОИБ. Также, по всем фактам, касающимся обработки и защиты персональных данных, в том числе, по фактам нарушениям законодательства в данной области, следует обращаться в ОИБ:

73-44-55

10-38

Благодарю за внимание!