

КОПИЯ

Министерство образования и науки Российской Федерации
(МИНОБРНАУКИ РОССИИ)

Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
«ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ УПРАВЛЕНИЯ»

ПРИКАЗ

«17» июня 2014г.

Москва

№ 244/14-И

Об утверждении Положения о защите персональных данных работников федерального государственного бюджетного образовательного учреждения высшего профессионального образования «Государственный университет управления»

В соответствии с Главой 14 Трудового кодекса Российской Федерации,

ПРИКАЗЫВАЮ:


1. Утвердить Положение о защите персональных данных работников федерального государственного бюджетного образовательного учреждения высшего профессионального образования «Государственный университет управления» (далее – Положение).
2. Начальнику Отдела кадров Б.В. Петренко ознакомить работников с Положением под роспись в срок до 1 сентября 2014 г.
3. Положение о защите, хранении, обработке и передачи персональных данных работников университета, утвержденное Ректором 24 ноября 2004 г. признать утратившим силу.
4. Контроль за исполнением настоящего приказа возложить на начальника Отдела кадров Б.В. Петренко.

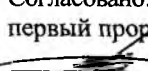
И.о. ректора




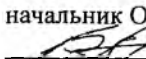
В.В. Годин

Проект приказа вносит:
начальник Управления правового
обеспечения


С.В. Райх

Согласовано:
первый проректор
 В.М. Свистунов

проректор
 В.В. Лобачев

начальник Отдела кадров
 Б.В. Петренко

УТВЕРЖДЕНО
приказом и.о. ректора
от «17» июля 2014 г.
№ 244/17-1

Положение о защите персональных данных работников
федерального государственного бюджетного образовательного учреждения
высшего профессионального образования
«Государственный университет управления»

Москва
2014

1. Общие положения

1.1. Положение о защите персональных данных работников федерального государственного бюджетного образовательного учреждения высшего профессионального образования «Государственный университет управления» (далее – Положение) разработано в соответствии с законодательством Российской Федерации и локальными нормативными актами федерального государственного бюджетного образовательного учреждения высшего профессионального образования «Государственный университет управления» (далее – ГУУ).

1.2. Целью Положения является установление порядка хранения, получения, обработки, использования, защиты (далее при использовании вместе – защита) персональных данных работников ГУУ от несанкционированного доступа, неправомерного их использования или утраты.

1.3. Персональные данные относятся к категории конфиденциальной информации. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении 75 лет срока хранения, если иное не определено законодательством Российской Федерации.

1.4. Действие настоящего Положения не распространяется на отношения, возникающие при организации хранения, комплектования, учета и использования содержащих персональные данные документов архивного фонда ГУУ.

1.5. Настоящее Положение является обязательным для исполнения всеми работниками ГУУ.

1.6. Работники должны быть ознакомлены под роспись с настоящим Положением.

2. Понятие и состав персональных данных

2.1. Персональные данные работника - информация, необходимая ГУУ, как работодателю для выполнения заявленной деятельности и касающаяся прямо или косвенно конкретного работника (субъекта персональных данных). Под информацией о работниках понимаются сведения о фактах, событиях и обстоятельствах жизни работника, позволяющие идентифицировать его личность. Персональные данные хранятся на бумажном (оригинал и/или копия) или электронном носителе (далее – носитель). Персональные данные работника, хранящиеся на электронных носителях, должны быть защищены паролем.

Пароль для персональных данных всех работников ГУУ, хранящихся на электронных носителях сообщается:

- ректору;
- начальнику Отдела кадров;
- начальнику Управления безопасности;

- директору Центра новых информационных технологий.

Пароль для персональных данных работников только своего подразделения, хранящихся на электронных носителях сообщается:

- проректорам по направлению деятельности;
- руководителям структурных подразделений и заместителям руководителей структурных подразделений.

Пароль для персональных данных работников в пределах участков работы, хранящихся на электронных носителях сообщается:

- руководителям структурных подразделений и заместителям руководителей структурных подразделений, работники которых имеют доступ к персональным данным в пределах своих участков работы.

2.2. В состав персональных данных работника, в том числе, входят:

- анкетные, паспортные и биографические данные, сведения об образовании, стаже, составе семьи, месте работы (учебы) членов семьи, воинском учете работника и наличии судимости;
- сведения о заработной плате, социальных льготах;
- условия трудового договора;
- декларируемые сведения о наличии материальных ценностей, содержание декларации, подаваемой в налоговую инспекцию;
- оригиналы и копии приказов по личному составу, основания к приказам по личному составу, личное дело и трудовая книжка работника;
- материалы по повышению квалификации, профессиональной переподготовке, аттестации работника, служебным расследованиям;
- копии отчетов, направляемые в органы статистики и иные государственные, муниципальные органы и органы местного самоуправления;
- иная информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу.

2.3. Документы и сведения, указанные в п. 2.2. настоящего Положения, являются конфиденциальными. Учитывая их массовость и единое место обработки и хранения - соответствующий гриф ограничения на них может не ставиться.

2.4. Все лица, обеспечивающие защиту персональных данных, обязаны подписать обязательство о неразглашении персональных данных работников (Приложение 1), которое хранится у начальника Отдела кадров.

3. Обработка персональных данных

3.1. Под обработкой персональных данных работника понимается 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.

3.2. Работники ГУУ занимающиеся обработкой персональных данных обязаны соблюдать следующие общие требования:

3.2.1. Обработка персональных данных работника может осуществляться исключительно в целях обеспечения содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

3.2.2. При определении объема и содержания обрабатываемых персональных данных необходимо руководствоваться законодательством Российской Федерации и локальными нормативными актами ГУУ.

3.2.3. Получение персональных данных может осуществляться как путем представления их самим работником, так и путем получения их из иных источников.

3.2.4. Персональные данные предпочтительно получать у самого работника. Если персональные данные работника необходимо получить из других источников, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие (Приложение 2). ГУУ 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.

3.2.5. ГУУ не имеет права получать и обрабатывать персональные данные работника о его политических, религиозных и иных убеждениях и частной жизни (сведения о его происхождении, о месте его пребывания или жительства, о личной и семейной, бытовой жизни). В случаях, непосредственно связанных с вопросами трудовых отношений, данные о частной жизни работника могут быть получены и обработаны только с его письменного согласия.

ГУУ не имеет право получать и обрабатывать персональные данные работника о его членстве в профсоюзе или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральными законами, о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции.

3.3. К персональным данным работника имеют доступ:

3.3.1. Право полного доступа:

- ректор;
- начальник Отдела кадров, заместители начальника Отдела кадров;
- начальник Управления безопасности, заместители начальника Управления безопасности;
- начальник Управления правового обеспечения, заместители начальника Управления правового обеспечения и начальники отделов Управления правового обеспечения.

3.3.2. Право ограниченного доступа:

3.3.2.1. Доступ к персональным данным работников только своего подразделения:

- проректоры по направлению деятельности, руководители и заместители руководителей структурных подразделений.

3.3.2.2. Доступ к персональным данным работников в пределах своих участков работы:

- работники структурных подразделений в рамках исполнения должностных обязанностей.

3.3.2.3. Доступ по запросу (Приложение 3):

- иные работники ГУУ при выполнении ими отдельных поручений ректора.

3.4. Контрольно-надзорные органы Российской Федерации имеют доступ к персональным данным работников ГУУ только в сфере своей компетенции.

Сведения о работнике, в том числе уволенном могут быть предоставлены другому юридическому лицу или индивидуальному предпринимателю только по письменному запросу с приложением нотариально заверенного согласия работника.

3.5. Лицам, имеющим право полного доступа, персональные данные предоставляются руководителем структурного подразделения, где хранится носитель, в течение одного часа после получения требования о предоставлении таких данных. Возврат оригинала носителя осуществляется в тот же или на следующий день за днем затребования, руководителю структурного подразделения, где хранится носитель.

На выходные (праздничные) дни оригинал носителя персональных данных возвращается руководителю структурного подразделения, где хранится носитель.

3.6. Лицам, имеющим право ограниченного доступа, персональные данные предоставляются руководителем структурного подразделения, где хранится носитель, в течение рабочего дня, а в исключительных случаях в течение одного часа, после получения письменного требования о предоставлении или запроса о доступе к персональным данным, при наличии положительной резолюции ректора соответственно (если это не связано с участком работы). Возврат оригинала носителя производится по мере завершения работы с носителем (но не позже трех дней после получения), руководителю структурного подразделения, где хранится носитель.

На выходные (праздничные) дни оригинал носителя персональных данных возвращается руководителю структурного подразделения, где хранится носитель.

3.7. Работники структурных подразделений ГУУ, где хранятся носители персональных данных, ведут Журнал учета выдачи носителей (далее – Журнал) (Приложение 4). Лицо, затребовавшее носитель обязано расписаться в Журнале о получении носителя и о его возврате.

3.8. Использование персональных данных возможно только в соответствии с целями, определившими их получение.

3.9. Персональные данные не могут быть использованы в целях причинения имущественного и морального вреда гражданам, затруднения реализации прав и свобод граждан Российской Федерации. Ограничение прав граждан Российской Федерации на основе использования информации об их социальном происхождении, о расовой, национальной, языковой, религиозной и партийной принадлежности запрещено и преследуется в соответствии с законодательством Российской Федерации.

3.10. Для защиты персональных данных работника должны соблюдаться следующие требования:

- запрещается предоставление персональных данных работника без его письменного согласия, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в случаях, установленных законодательством Российской Федерации;

- запрещается предоставление и использование персональных данных работника в коммерческих целях без его письменного согласия;

- необходимо предупреждать лицо, получающее персональные данные работника, о том, что персональные данные могут быть использованы лишь в целях, для которых эти данные были затребованы;

- выдача разрешения ректором на доступ или передачу персональных данных работников, лицам, не имеющим права доступа к персональным данным, в соответствии с данным Положением.

3.11. Все меры конфиденциальности при защите персональных данных работника распространяются как на бумажные, так и на электронные (автоматизированные) носители информации.

3.12. Не допускается передача персональных данных по телефону, факсу, в сети Интернет.

3.13. Защита персональных данных должна происходить в порядке, исключающем их утрату или их неправомерное использование.

3.14. При необходимости блокирование и удаление персональных данных производится на основании приказа ректора.

3.15. Уничтожение персональных данных производится по Акту уничтожения носителя персональных данных (далее – Акт) (Приложение 5), подписанному ректором или иным уполномоченным лицом с соблюдением требований архивного дела. Уничтожение бумажных и электронных носителей производится механическим путем, путем разрезания, сжигания, сдачи предприятию по утилизации вторичного сырья, способ указывается в Акте.

4. Защита персональных данных

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

4.2. 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.

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

4.4. Регламентация доступа к конфиденциальным сведениям, документам и базам данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий между руководителями и иными работниками ГУУ.

4.5. Для обеспечения защиты персональных данных работников необходимо соблюдать ряд мер:

- строгое избирательное и обоснованное распределение документов и информации между работниками;
- рациональное размещение рабочих мест работников, при котором исключалось бы бесконтрольное использование защищаемой информации;
- знание работником требований нормативных правовых актов по защите информации;
- 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 которых происходит защита персональных данных;
- организация порядка уничтожения информации;
- своевременное выявление нарушений требований разрешительной системы доступа работниками;
- воспитательная и разъяснительная работа с работниками по предупреждению утраты персональных данных при работе с конфиденциальными документами.

4.6. Для обеспечения защиты персональных данных работников необходимо соблюдать ряд мер:

- регламентированный порядок приема, учета и контроля деятельности посетителей;

- пропускной режим в ГУУ;

- учет и порядок выдачи удостоверений работникам и пропусков в ГУУ;

- наличие технических средств охраны, сигнализации.

4.7. По возможности, персональные данные обезличиваются.

4.8. Кроме мер защиты персональных данных, установленных законодательством Российской Федерации, работодатели, работники и их представители могут вырабатывать совместные меры защиты персональных данных работников.

4.9. В целях защиты персональных данных, хранящихся в ГУУ, работник имеет право:

- получать информацию, касающуюся обработки его персональных данных, в том числе подтверждение факта обработки персональных данных, правовые основания и цели обработки персональных данных, сроки обработки персональных данных, в том числе сроки их хранения и иные сведения, предусмотренные законодательством Российской Федерации по защите персональных данных;

- требовать исключения или исправления неверных или неполных персональных данных;

- получать свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные;

- дополнять персональные данные оценочного характера заявлением, выражающим его собственную точку зрения;

- определять своих представителей для защиты своих персональных данных;

- обжаловать действия или бездействие ответственных за обработку персональных данных структурных подразделений ГУУ.

5. Ответственность за разглашение персональных данных

5.1. Работник, имеющий доступ к персональным данным несет ответственность за сохранность носителя и конфиденциальность информации, содержащей персональные данные. Персональная ответственность - одно из главных требований к организации функционирования системы защиты персональной информации и обязательное условие обеспечения эффективности этой системы.

5.2. Лица, виновные в нарушении норм, регулирующих защиту персональных данных работника, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством Российской Федерации.

Обязательство
о неразглашении персональных данных

Я, _____,
зарегистрированный/ая по адресу _____

Паспорт _____, выдан _____

_____ понимаю, что получаю доступ к персональным данным работников федерального государственного бюджетного образовательного учреждения высшего профессионального образования «Государственный университет управления» (далее – ГУУ), а также понимаю, что во время исполнения своих обязанностей занимаюсь сбором, обработкой и хранением персональных данных работников.

Я понимаю, что разглашение такого рода информации может нанести ущерб работникам ГУУ, как прямой, так и косвенный.

В связи с этим даю обязательство при работе (сборе, обработке и хранении) с персональными данными работников соблюдать требования Положения о защите персональных данных работников ГУУ.

Я предупрежден (а) о том, что в случае разглашения мной сведений, касающихся персональных данных работника, или их утраты я несу ответственность в соответствии со статьей 90 Трудового кодекса Российской Федерации.

С Положением о защите персональных данных работников федерального государственного бюджетного образовательного учреждения высшего профессионального образования «Государственный университет управления» ознакомлен (а).

_____ (должность)
« ____ » _____ 201_ г.

_____ (ФИО)

Согласие
на получение, обработку и хранение персональных данныхЯ, _____,
зарегистрированный/ая по адресу _____Паспорт _____, выдан _____
(серия, номер) (когда и кем выдан)

(далее – Работник) даю согласие федеральному государственному бюджетному образовательному учреждению высшего профессионального образования «Государственный университет управления» (далее – ГУУ), расположенному по адресу 109542, г. Москва, Рязанский проспект, д.99, на получение, обработку и хранение моих персональных данных, таких как: Фамилия, Имя, Отчество; дата (число, месяц, год) рождения; пол; гражданство; адрес постоянной и временной (при наличии последней) регистрации; данные документа, удостоверяющего личность; данные об имеющихся уровнях образования; данные о трудовой деятельности (трудовая книжка); контактная информация (адрес, номер(а) телефона(ов), e-mail); фото; иные персональные данные Работника, необходимые для целей Работодателя в рамках действующего законодательства.

Персональные данные предоставляются для их хранения и обработки в общедоступные источники информации в рамках функционирования информационных систем обеспечения и мониторинга учебного процесса, научной, организационной, финансово-экономической и иной деятельности Работодателя, предусмотренной Уставом ГУУ, различные базы данных и информационные системы, Интернет, включения их в аналитические и статистические отчетности.

ГУУ имеет право передать указанные данные для использования их способами, указанными во втором абзаце третьим лицам, в соответствии с Положением о защите персональных данных работников федерального государственного бюджетного образовательного учреждения высшего профессионального образования «Государственный университет управления».

Отзыв согласия на получение, обработку и хранение персональных данных производится Работником путем направления соответствующего письменного уведомления ГУУ. Отзыв начинает действовать с момента его получения ГУУ.

Работник _____
(подпись)

_____ (ФИО)

« _____ » _____ 20 ____ г.

(наименование структурного подразделения)

И.о. ректора
В.В. Годину**Запрос**

«__» _____ 201__ г. № _____

Уважаемый Владимир Викторович!

Прошу Вас разрешить единовременный доступ к персональным
данным _____

(ФИО, должность, структурное подразделение)

хранящимся в _____

(наименование структурного подразделения)

в целях _____

Начальник структурного подразделения _____

(подпись)

(ФИО)

Обязательство о неразглашении персональных данных от
«__» _____ 20__ г. хранится в личном деле работника.

Работник Отдела кадров _____

(подпись)

(ФИО)

Журнал учета выдачи носителей

№ п/п	Дата	Тип носителя и краткое содержание персональных данных	Структурное подразделение, должностное лицо запросившее персональные данные	Получил (ФИО, подпись)	Вернул (ФИО, подпись, дата)

Акт уничтожения носителя персональных данных

Комиссия, наделенная полномочиями приказом ректора __ от ____ №
____, в составе:

	ФИО	Должность
Председатель		
Члены комиссии		

провела отбор носителей персональных данных и установила, что информация, записанная на них в процессе эксплуатации, подлежит гарантированному уничтожению:

№ п/п	Дата	Тип носителя	Регистрационный номер носителя	Примечание

Всего съемных носителей _____

(цифрами и прописью)

На указанных носителях персональные данные уничтожены путем

_____ (стирания на устройстве гарантированного уничтожения информации и т.п.)

Перечисленные носители персональных данных уничтожены путем

_____ (разрезания, сжигания, механического уничтожения, сдачи предприятию по утилизации вторичного сырья и т.п.)

Председатель комиссии:

_____ (подпись)

_____ (ФИО)

Члены комиссии:

_____ (подпись)

_____ (ФИО)

_____ (подпись)

_____ (ФИО)