Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Целищев Алексей Олегович
Должность: Проректор по учебно-научной работе
Дата подписания: 08.07.2025 13:20:23
Уникальный программный ключ:
a8cad4623edd7219a3b0897308bb14769288026a

Приложение № 1 к приказу
от « 18 »июня 2025 г. №112/к

ПОЛОЖЕНИЕ
об обработке персональных данных в Академии ВЭГУ

1 Общие положения

1.1 Термины и определения

1.1.1 Персональные данные (ПДн) – любая информация, относящаяся к прямо или косвенно определённому или определяемому физическому лицу (субъекту персональных данных).

1.1.2 Обработка персональных данных – 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.

1.1.3 Распространение персональных данных – действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

1.1.4 Использование персональных данных – действия с персональными данными, совершаемые субъектом персональных данных частного образовательного учреждения высшего образования «Восточная экономико-юридическая гуманитарная академия» (Далее - Академия, Работодатель) в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

1.1.5 Автоматизированная обработка – обработка данных, выполняемая средствами вычислительной техники.

1.1.6 Блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи.

1.1.7 Уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

1.1.8 Обезличивание персональных данных – действия, в результате которых

невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

1.1.9 Информационная система персональных данных – система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

1.1.10 Защита персональных данных – деятельность уполномоченных лиц по обеспечению с помощью локального регулирования порядка обработки персональных данных и организационно-технических мер конфиденциальности информации о конкретном субъекте персональных данных.

1.2 Назначение и правовая основа документа.

1.2.1 Настоящее Положение об обработке персональных данных (далее – Положение) определяет порядок получения, хранения, обработки, комбинирования, передачи и любого другого использования персональных данных Академии в соответствии с законодательством Российской Федерации.

1.2.2 Настоящее Положение разработано в соответствии с:

- Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (с изменениями и дополнениями);
- Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» » (с изменениями и дополнениями);
- Постановление Правительства РФ от 15 сентября 2008 г. N 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» (с изменениями и дополнениями).
- Иными законодательными и нормативными правовыми актами РФ, регламентирующими порядок работы с персональными данными.

2 Получение, обработка и защита персональных данных

2.1 Порядок получения персональных данных

– все персональные данные следует получать лично у субъекта ПДн. Если персональные данные, возможно, получить только у третьей стороны, то субъект ПДн должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Академия должно сообщить субъекту ПДн о целях, предполагаемых источниках и способах получения персональных данных, характере подлежащих получению персональных данных и последствиях отказа субъекта ПДн дать письменное согласие на их получение;

– Академия вправе обрабатывать персональные данные субъектов ПДн только с их письменного разрешения;

– письменное согласие субъекта ПДн на обработку своих персональных данных должно включать в себя персональные данные, указанные в перечне ПДн, подлежащих защите в ИСПДн;

– Академия не имеет права получать и обрабатывать персональные данные субъекта ПДн о его политических, религиозных и иных убеждениях, частной жизни, членстве в

общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных законодательством Российской Федерации;

– работники Академии имеют право получать только те ПДн, которые необходимы им для выполнения своих служебных обязанностей;

– работники Академии, получающие персональные данные субъекта ПДн, обязаны соблюдать режим конфиденциальности.

2.2 Порядок обработки персональных данных.

2.2.1 Обработка персональных данных может осуществляться Академией с письменного согласия субъектов ПДн, за исключением случаев, предусмотренных федеральным законом.

2.2.2 Обработка персональных данных может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия субъекту ПДн в трудоустройстве, обучении, продвижении по службе, обеспечения личной безопасности субъекта ПДн, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

2.2.3 Все персональные данные субъекта ПДн следует получать от него самого. Если персональные данные субъекта ПДн можно получить только у третьей стороны, то субъект ПДн должен быть уведомлен об этом заранее, и от него должно быть получено письменное согласие. Академия должна сообщить субъекту ПДн о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа субъекта ПДн дать письменное согласие на их получение.

2.2.4 Нельзя получать и обрабатывать персональные данные субъекта ПДн о его политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьей 24 Конституции Российской Федерации Работодатель вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия.

2.2.5 Персональные данные не могут быть использованы в целях причинения имущественного и/или морального вреда гражданам, затруднения реализации прав и свобод граждан Российской Федерации.

2.2.6 Защита персональных данных субъекта ПДн от неправомерного их использования или утраты должна быть обеспечена за счет средств Академии в порядке, установленном законодательством Российской Федерации.

2.2.7 Все субъекты ПДн должны быть ознакомлены с документами организации, устанавливающими порядок обработки персональных данных субъекта ПДн, а также об их правах и обязанностях в этой области.

2.2.8 Субъекты ПДн не должны отказываться от своих прав на сохранение и защиту конфиденциальности своих персональных данных и иных видов тайн, предусмотренных законодательством.

2.3 Порядок защиты персональных данных.

– защита персональных данных субъекта ПДн от неправомерного их использования или утраты должна быть обеспечена Академией за счет собственных средств в порядке,

установленном федеральными законами Российской Федерации в области защиты персональных данных;

– Академия обязана при обработке персональных данных субъектов персональных данных принимать необходимые организационные и технические меры для защиты персональных данных от несанкционированного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий;

– соблюдать порядок получения, учета и хранения персональных данных субъектов ПДн;

– применять технические средства охраны и сигнализации;

– взять со всех работников, связанными с получением, обработкой и защитой персональных данных субъектов ПДн, Обязательство о неразглашении персональных данных;

– привлекать к дисциплинарной ответственности работников, виновных в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта ПДн;

– запретить допуск к персональным данным субъектов ПДн работников Академии, не включенных в ПЕРЕЧЕНЬ должностей работников, допущенных к работе с ПДн;

– защита доступа к электронной базе данных, содержащей персональные данные субъектов ПДн, должна обеспечиваться путем использованием сертифицированных программных и программно-аппаратных средств защиты информации, предотвращающих несанкционированный доступ третьих лиц к персональным данным субъектов ПДн;

– копировать и делать выписки персональных данных субъектов ПДн разрешается исключительно в служебных целях;

– субъекты ПДн не должны отказываться от прав на сохранение и защиту своих персональных данных;

– Академия, субъекты ПДн и их представители должны совместно вырабатывать меры защиты персональных данных субъектов ПДн.

3 Хранение, передача, доступ к персональным данным

3.1 При передаче персональных данных субъекта ПДн Академия должна соблюдать следующие требования:

– при передаче персональных данных субъекта ПДн использовать выделенную WAN (глобальную компьютерную сеть) с применением сертифицированных средств криптографической защиты информации;

– не сообщать персональные данные субъекта ПДн третьей стороне без письменного согласия субъекта ПДн, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в случаях, предусмотренных Трудовым Кодексом Российской Федерации или иными федеральными законами;

– передавать персональные данные субъекта ПДн представителю субъекта ПДн в порядке, установленном федеральными законами Российской Федерации.

– не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции;

3.2 Сведения о субъектах ПДн в Академии на бумажных носителях должны храниться в специально оборудованных шкафах и сейфах, которые запираются и/или опечатываются. Ключи от шкафов и сейфов, в которых хранятся сведения о субъектах ПДн, находятся у ответственных за хранилища. Сведения, относящиеся к персональным данным, хранятся в личном деле.

3.3 Личные дела хранятся:

– в бумажном виде в папках, прошитые и пронумерованные по страницам;

– в алфавитном порядке;

– в специально отведенных запираемых шкафах (отдельных запираемых помещениях), обеспечивающих защиту от несанкционированного доступа.

3.4 Трудовые книжки на бумажных носителях работников хранятся в сейфах отдела кадров, доступ к которому имеют только начальник отдела кадров и специалисты отдела кадров, отвечающие за ведение трудовых книжек. Хранение трудовых книжек работников осуществляется в соответствии с Правилами ведения и хранения трудовых книжек, изготовления бланков трудовых книжек и обеспечения ими работодателей, утвержденными Постановлением Правительства Российской Федерации.

3.5 Ответственность за хранение сведений о субъектах ПДн, заполнение, хранение и выдачу документов, содержащих персональные данные, в ИСПДн возлагаются на Ответственного за организацию обработки персональных данных.

3.6 Съемные электронные носители, на которых хранятся резервные копии персональных данных субъектов ПДн, должны быть промаркированы и учтены в журнале регистрации, учета и выдачи внешних носителей для хранения резервных копий ПДн.

3.7 В процессе хранения персональных данных субъектов ПДн необходимо обеспечивать контроль за достоверностью и полнотой персональных данных, их регулярное обновление и внесение по мере необходимости соответствующих изменений.

3.8 К числу массовых потребителей персональных данных вне Академии ВЭГУ относятся государственные и негосударственные функциональные структуры, в том числе налоговые; правоохранительные органы; служба судебных приставов; военкоматы; социальный фонд России и т.п.. Контрольно-надзорные органы имеют доступ к информации только в сфере своей компетенции.

3.9 Персональные данные, включенные в информационные справочники Академии, являются общедоступными.

3.10 Персональные данные работников Академии могут предоставляться в соответствующие организации для оформления проездных документов и размещения в местах проживания в случае служебных командировок.

3.11 Персональные данные работников Академии могут предоставляться в образовательные учреждения в случае направления работника на учебу, а также в соответствующие организации для участия в выставках, конференциях и семинарах и т.п..

3.12 Организации, в которые работник может осуществлять перечисления денежных средств (страховые общества, негосударственные пенсионные фонды, благотворительные организации, кредитные учреждения) могут получить доступ к персональным данным работника только в случае его письменного согласия.

4 Уничтожение персональных данных

4.1 При необходимости уничтожения персональных данных Академия должна руководствоваться следующими требованиями:

– уничтожение персональных данных в ИСПДн осуществляется комиссией по проведению мероприятий по защите персональных данных;

– бумажные носители персональных данных должны уничтожаться при помощи специального оборудования (измельчителя бумаги);

– персональные данные, представленные в электронном виде, должны уничтожаться специализированным программным обеспечением, гарантирующим предотвращение восстановления удаленных данных;

– после окончания процедуры удаления персональных данных комиссией по проведению мероприятий по защите персональных данных должен быть составлен акт уничтожения персональных данных.

5 Внутренние проверки состояния защищенности информационной системы персональных данных

5.1 Проверка состояния защищенности ИСПДн осуществляется комиссией по проведению мероприятий по защите персональных данных.

5.2 Проверка состояния защищенности ИСПДн осуществляется с целью определения соответствия нормативных, организационных, практических и технических мероприятий, реализуемых Академией, требованиям законов и иных нормативных правовых актов Российской Федерации в области информационной безопасности и защиты персональных данных.

5.3 Проверка состояния защищенности ИСПДн включает в себя:

– определение характера циркулирующих персональных данных и установленных в ИСПДн режимов их обработки;

– определение актуальности организационно-распорядительной документации, учитывающей конкретные условия функционирования средств вычислительной техники различного уровня и назначения (рабочие станции пользователей, серверное и периферийное оборудование, технические средства защиты информации, в том числе средства криптографической защиты информации), порядок работы сотрудников организации при эксплуатации средств вычислительной техники;

– анализ принятых мер (программных, технических, организационных), обеспечивающих защиту средств вычислительной техники, информационной системы и баз данных от несанкционированного доступа, оценка продуктивности организационного процесса защиты информации. Достаточность технических средств обработки и защиты информации, наличие подтверждений соответствия по требованиям информационной безопасности (сертификатов соответствия);

– проведение анализа конфигураций активного сетевого оборудования, маршрутизаторов, коммутаторов, серверов с целью выявления уязвимых мест в системе защиты информации;

– проведение инструментального анализа сетевого и серверного оборудования локально-вычислительных сетей, информационных систем и баз данных с применением программно-аппаратных средств;

– проверка работоспособности используемых программных и программно-аппаратных средств обнаружения и предотвращения компьютерных атак;

– проверка наличия лицензионных средств защиты от вредоносных программ и вирусов или сертифицированных свободно распространяемых антивирусных средств защиты;

– проверка оснащения серверных и кроссовых помещений средствами контроля доступа и пожаротушения, обеспечения температурного режима, регламент доступа к серверным и кроссовым помещениям;

– проверка состояния защищенности информационных ресурсов от сбоев в системе электропитания (система резервирования и автоматического ввода резерва);

– проверка состояния линейно-кабельного оборудования локально-вычислительных сетей (наличие запирающих и опечатывающих устройств, оборудования распределительных шкафов).

5.4 Внутренняя проверка Комиссии по проведению мероприятий по защите персональных данных завершается подведением итогов (обобщением) результатов проверки и составлением акта о результате проверки состояния защищенности ИСПДн.

5.5 Акт должен содержать:

– дата, время и место составления акта;

– дата и место проведения проверки;

– сведения о результатах проверки, в том числе о выявленных нарушениях и их характере;

– достоверное и обоснованное изложение состояния защищенности информационной системы и ресурсов, выявленных недостатков и нарушений со ссылками на соответствующие документы и факты, выводы и предложения по их устранению с указанием конкретных сроков.

6 Обязанности субъекта персональных данных и Академии

6.1 В целях обеспечения достоверности персональных данных субъект ПДн обязан:

– предоставлять Академии полные и достоверные данные о себе;

– в случае изменения своих персональных данных сообщать данную информацию Академии.

Академия обязана:

– осуществлять защиту персональных данных субъекта ПДн;

– вести Журнал учета обращений субъектов персональных данных по вопросам обработки их ПДн в ИСПДн;

– обеспечивать хранение документации, содержащей персональные данные субъектов ПДн, при этом персональные данные не должны храниться дольше, чем это оправдано выполнением задач, для которых они собирались, или дольше, чем это требуется в интересах лиц, о которых собраны данные.

7 Права субъекта ПДн в целях защиты персональных данных

7.1 Субъект персональных данных вправе требовать от Оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

7.2 Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

- подтверждение факта обработки персональных данных Оператором;
- правовые основания и цели обработки персональных данных;
- цели и применяемые Оператором способы обработки персональных данных;
- сроки обработки персональных данных, в том числе сроки их хранения.

7.3 Субъект персональных данных имеет право на определение представителей для защиты своих персональных данных.

7.4 Субъект персональных данных имеет право требовать исключить или исправить неверные или неполные персональные данные, а также данные, обрабатываемые с нарушением требований Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

7.5 Субъект персональных данных имеет право требовать об извещении Академией всех лиц, которым ранее были сообщены неверные или неполные персональные данные субъекта ПДн, обо всех произведенных в них исключениях, исправлениях или дополнениях.

7.6 Субъект персональных данных имеет право на обжалование в судебном порядке любых неправомерных действий или бездействии Академии при обработке и защите его персональных данных.

8 Ответственность за нарушение норм, регулирующих получение, обработку и защиту персональных данных субъекта ПДн

8.1 Лица, виновные в нарушении требований федеральных законов РФ, несут предусмотренную законодательством РФ ответственность.

8.2 Моральный вред, причиненный субъекту ПДн вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных федеральными законами, а также нарушения требований к защите персональных данных подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.