УТВЕРЖДЕНО
на заседании Ученого совета
29 августа 2019 г., протокол №1
Председатель Ученого Совета,
ректор института
_____ А.А. Егоров

ПОЛОЖЕНИЕ
О ЗАЩИТЕ, ХРАНЕНИИ, ОБРАБОТКЕ И ПЕРЕДАЧИ ДАННЫХ ОБУЧАЮЩИХСЯ, РАБОТНИКОВ УВО МХПИ

Москва, 2019

1. Общие положения

1.1. Целью данного Положения является защита персональных данных обучающихся и абитуриентов Учреждения высшего образования «Московский художественно-промышленный институт» (далее УВО МХПИ, МХПИ, институт) от несанкционированного доступа, неправомерного их использования или утраты.

1.2. Настоящее Положение разработано на основании статей Конституции РФ, Трудового кодекса РФ, Кодекса РФ об административных правонарушениях, Гражданского кодекса РФ, Уголовного кодекса РФ, а также Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», и других действующих нормативно-правовых актов Российской Федерации.

1.3. Персональные данные относятся к категории конфиденциальной информации. Режим конфиденциальности персональных данных снимается в случаях обезличивания персональных данных, по истечении срока хранения, если иное не определено законом, и в отношении общедоступных персональных данных.

1.4. Настоящее Положение утверждается Ученым советом и вводится в действие приказом Ректора, является обязательным для исполнения всеми работниками, имеющими доступ к персональным данным обучающихся, абитуриентов.

2. Понятие и состав персональных данных

2.1. В настоящем Положении используются следующие термины и определения:

Персональные данные - это любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, имущественное положение, образование, профессия, доходы, а также сведения о фактах, событиях и обстоятельствах жизни обучающегося или абитуриента, позволяющая идентифицировать его личность.

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.

Сбор персональных данных – накопление информации на материальных носителях и (или) в автоматизированных информационных системах.

Хранение персональных данных – комплекс мероприятий, направленный на обеспечение сохранности полноты и целостности сформированных массивов персональных данных, создание и поддержание

надлежащих условий для их использования, а также предупреждение несанкционированного доступа, распространения и использования.

Общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

Согласие субъекта персональных данных – свободно данное конкретное и сознательное указание о своей воле, которым субъект персональных данных оповещает о своем согласии на обработку касающихся его персональных данных.

Третья сторона – любое физическое или юридическое лицо, орган государственной власти или местного самоуправления, кроме субъекта персональных данных, университета (оператора) и лиц, уполномоченных на получение, обработку, хранение, передачу и другое использование персональных данных на законных основаниях.

Защита персональных данных – технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и обеспечивающий безопасность информации в процессе деятельности Института.

Материальный носитель – бумажный и машиночитаемый носители информации (в том числе магнитный и электронный), на которых осуществляются запись и хранение сведений, на основе которых можно установить личность физического лица.

Доступ к персональным данным – возможность получения персональных данных и их использования.

Несанкционированный доступ – доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своим функциональному предназначению и техническим характеристикам.

База данных – объективная форма представления и организации совокупности данных (например, статей, расчётов), систематизированных таким образом, чтобы эти данные могли быть найдены и обработаны с помощью ЭВМ.

2.2**. В состав персональных данных абитуриента входят:**

-персональные данные, содержащиеся в заполненном заявлении о приеме;

-сведения о результатах ЕГЭ;

-сведения о льготах;

-фотографии для личного дела;

-гражданство;

-прочие документы, в том числе характеристики, направления, сведения о наградах и т.п.

2.3**. В состав персональных данных работника, обучающегося** (студенты всех форм обучения, слушатели курсов повышения квалификации и дополнительных образовательных программ) входят:

- фамилия, имя, отчество;

- дата и место рождения;
- сведения документов, удостоверяющих личность;
- адрес места жительства (фактический, по регистрации);
- телефонный номер;
- e-mail;
- успеваемость, характеристики, награды, достижения;
- сведения о трудовой деятельности;
- медицинские сведения; гражданство;
- доходы;
- сведения о семье;
- сведения об образовании;
- сведения о воинском учёте;
- сведения о пенсионном страховании;
- сведения о налоговом учёте;
- сведения о счетах в банках; фотоматериалы.

3. Обработка персональных данных

3.1. Под обработкой персональных данных обучающегося, абитуриента понимаются действия (операции), включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

3.2. В целях обеспечения прав и свобод человека и гражданина Институт при обработке персональных данных обучающегося, абитуриента обязан соблюдать следующие общие требования:

3.2.1. Обработка персональных данных может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия обучающимся в трудоустройстве, обучении, обеспечения личной безопасности обучающихся, абитуриентов, контроля количества и качества выполняемой работы в результате образовательного процесса и обеспечения сохранности имущества.

3.2.2. При определении объема и содержания обрабатываемых персональных данных Институт должен руководствоваться Конституцией Российской Федерации, Трудовым кодексом и иными федеральными законами.

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

3.2.4. Персональные данные следует получать у самого обучающегося, абитуриента, работника. Если персональные данные возможно получить только у третьей стороны, то работник, обучающийся или абитуриент должен быть уведомлен об этом заранее, и от него должно быть получено письменное согласие. Институт должен сообщить работнику, обучающемуся, абитуриенту о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и

последствиях отказа работника, обучающегося или абитуриента дать письменное согласие на их получение.

3.2.5. Институт не имеет права получать и обрабатывать персональные данные работника, обучающегося, абитуриента о его политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, данные о частной жизни (информация о жизнедеятельности в сфере семейных, бытовых, личных отношений) могут быть получены и обработаны работодателем только с его письменного согласия.

3.2.6. Институт не имеет право получать и обрабатывать персональные данные работника, обучающегося, абитуриента о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральными законами.

3.2.7. **Согласия работника, обучающегося, абитуриента не требуется** в случаях, если обработка персональных данных осуществляется:

- в целях исполнения договора, одной из сторон которого является работник, обучающийся, абитуриент;
- в целях исполнения требований законодательных требований по размещению информации в электронной информационно-образовательной среде и на официальном сайте образовательной организации;
- для статистических или иных научных целей при условии обязательного обезличивания персональных данных;
- для защиты жизни, здоровья или иных жизненно важных интересов работника, обучающегося, абитуриента, если получение согласия работника, обучающегося, абитуриента невозможно;
- в целях научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и свободы работника, обучающегося, абитуриента;
- в целях обеспечения развития и нормального функционирования Института, при этом из обрабатываемых персональных данных должны быть исключены паспортные данные, данные о месте рождения и проживания, семейном, имущественном положении, доходах и другая информация, которая при несанкционированном доступе к ней может принести материальный и/или моральный вред работнику, обучающемуся, абитуриенту;
- для осуществления правосудия;
- в целях соблюдения законодательства РФ о безопасности, об оперативно-розыскной деятельности, а также в соответствии с уголовно-исполнительным законодательством РФ.

3.3. К обработке, передаче и хранению персональных данных работника, обучающегося, абитуриента могут иметь доступ, сотрудники Института в соответствии с должностными инструкциями.

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

3.4.1. 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 о их расовой, национальной, языковой, религиозной и партийной принадлежности запрещено и карается в соответствии с законодательством.

3.5. Передача персональных данных работника, обучающегося, абитуриента возможна только с согласия работника, обучающегося, абитуриента или в случаях, прямо предусмотренных законодательством.

3.6. При передаче персональных данных работника, обучающегося, абитуриента Институт должен соблюдать следующие требования:

- не сообщать персональные данные работника, обучающегося, абитуриента третьей стороне без письменного согласия работника, обучающегося, абитуриента, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью, а также в случаях, установленных федеральным законом;

- не сообщать персональные данные работника, обучающегося, абитуриента в коммерческих целях без его письменного согласия;

- предупредить лиц, получающих персональные данные работника, обучающегося, абитуриента, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные работника, обучающегося, абитуриента, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется на обмен персональными данными обучающегося, абитуриента в порядке, установленном федеральными законами;

- разрешать доступ к персональным данным работника, обучающегося, абитуриента только специально уполномоченным лицам, определенным приказом по организации, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы для выполнения конкретных функций;

- не запрашивать информацию о состоянии здоровья работника, обучающегося, абитуриента, за исключением тех сведений, которые относятся к вопросу образовательного процесса и социальной помощи;

- передавать персональные данные представителям абитуриентов, обучающихся в порядке, установленном федеральным законодательством, и ограничивать эту информацию только теми персональными данными обучающегося, абитуриента, которые необходимы для выполнения указанными представителями их функций.

3.7. Все меры конфиденциальности при сборе, обработке и хранении персональных данных работников, обучающихся и абитуриентов распространяются как на бумажные, так и на электронные (автоматизированные) носители информации.

3.8. Не допускается отвечать на вопросы, связанные с передачей персональной информации по телефону или факсу.

3.9. Хранение персональных данных должно происходить в порядке, исключающем их утрату или их неправомерное использование.

3.10. При принятии решений, затрагивающих интересы обучающегося, абитуриента Институт не имеет права основываться на персональных данных

обучающегося, абитуриента, полученных исключительно в результате их автоматизированной обработки или электронного получения. Университет учитывает личные качества обучающегося, абитуриента, его добросовестный и эффективный труд в процессе обучения, образовательной подготовки.

4. Доступ к персональным данным

4.1. Внутренний доступ (доступ внутри Института).

4.1.1. Право доступа к персональным данным работников, обучающихся и абитуриентов, имеют:

- ректор Института;
- руководители структурных подразделений по направлению профиля обучения;
- сам работник, обучающийся, абитуриент носитель данных;
- другие сотрудники организации при выполнении ими своих служебных обязанностей.

4.1.2. Доступ к персональным данным обучающихся, других работников, хранящимся в институте, работник может получить на основании служебной записки, завизированной ректором или проректором по развитию и инновациям.

4.2. Внешний доступ.

4.2.1. К числу массовых потребителей персональных данных вне Института относятся:

- государственные и негосударственные функциональные структуры;
- налоговые инспекции;
- правоохранительные органы;
- органы статистики;
- страховые агентства;
- военкоматы;
- органы социального страхования;
- органы управления государственными внебюджетными фондами;
- государственные (в том числе органы государственной власти) и муниципальные органы.

4.2.2. Надзорно-контрольные органы имеют доступ к информации только в сфере своей компетенции.

4.2.3. Другие организации. Сведения работника, обучающегося, абитуриента могут быть предоставлены другой организации только с письменного запроса на бланке организации, с приложением копии нотариально заверенного заявления работника, обучающегося, абитуриента.

Персональные данные абитуриента, обучающегося могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого обучающегося, абитуриента.

5. Защита персональных данных

5.1. 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.

5.2. 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.

5.3. 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 Института.

5.4. Защита персональных данных работника, обучающегося, абитуриента от неправомерного их использования или утраты должна быть обеспечена Институтом за счет его средств в порядке, установленном федеральными законами.

5.5. «Внутренняя защита».

5.5.1. 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 Института.

5.5.2. Для обеспечения внутренней защиты персональных данных обучающихся, абитуриентов 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;
- хранение и учет подписанных сотрудниками, обрабатывающими персональные данные, обязательств о неразглашении персональных данных;
- рациональное размещение рабочих мест работников, при котором исключалось бы бесконтрольное использование защищаемой информации;
- знание работником требований нормативно-методических документов по защите информации и сохранении тайны;
- 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 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;
- не допускается выдача личных дел обучающихся. Личные дела могут выдаваться на рабочие места только ректору, проректору по учебной и

воспитательной работе и, в исключительных случаях на рабочие места иных сотрудников по письменному разрешению ректора, проректора по учебной и воспитательной работе.

5.5.3. Защита персональных данных работника, обучающегося, абитуриента на электронных носителях. Все данные на электронных носителях должны быть защищены паролями.

5.6. «Внешняя защита».

5.6.1. 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.

5.6.2. Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности Института, 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.

5.6.3. Для обеспечения внешней защиты персональных данных обучающихся, абитуриентов необходимо соблюдать ряд мер:

- порядок приема, учета и контроля деятельности посетителей;
- пропускной режим Института;
- учет и порядок выдачи карточек пропуска;
- технические средства охраны, сигнализации;
- порядок охраны территории, зданий, помещений;
- требования к защите информации при интервьюировании и собеседованиях.

5.7. Все лица, выполнение должностных обязанностей которых связанно с получением, обработкой и защитой персональных данных, обязаны подписать обязательство о неразглашении персональных данных.

5.8. По возможности персональные данные обезличиваются.

6. Права и обязанности обучающегося, абитуриента

6.1. Закрепление прав обучающегося, абитуриента регламентирующих защиту его персональных данных, обеспечивает сохранность полной и точной информации о нем.

6.2. В целях защиты персональных данных, хранящихся в Институте, обучающийся, абитуриент имеет право:

- требовать исключения или исправления неверных или неполных персональных данных;
- на свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные; - персональные данные оценочного характера дополнить заявлением, выражающим его собственную точку зрения;

- определять своих представителей для защиты своих персональных данных;

- на сохранение и защиту своей личной и семейной тайны,

- другие определенные законодательством права.

6.3. Обучающиеся, абитуриенты обязаны:

- передавать Институту или его представителю комплекс достоверных, документированных персональных данных, состав которых установлен Правилами приема в Институт;

- своевременно сообщать Институту об изменении своих персональных данных.

6.4. Обучающиеся ставят Институт в известность об изменении фамилии, имени, отчества, даты рождения, что получает отражение в личном деле. При необходимости изменяются данные об образовании, профессии, специальности и прочее.

6.5. Обучающийся, абитуриент имеет право на получение информации:

1) подтверждающей факт обработки персональных данных Института, а также цель такой обработки;

2) способы обработки персональных данных, применяемые в Институте;

3) сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;

4) перечень обрабатываемых персональных данных и источник их получения;

5) сроки обработки персональных данных, в том числе сроки их хранения;

6) сведения о том, какие юридические последствия для обучающегося, абитуриента может повлечь за собой обработка его персональных данных.

6.6. Право обучающегося, абитуриента на доступ к своим персональным данным ограничивается в случае, если:

- обработка персональных данных осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;

- обработка персональных данных осуществляется органами, осуществившими задержание обучающегося по подозрению в совершении преступления, либо предъявившими обучающемуся обвинение по уголовному делу, либо применившими к обучающемуся меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством Российской Федерации случаев, если допускается ознакомление подозреваемого или обвиняемого с такими персональными данными;

- предоставление персональных данных нарушает конституционные права и свободы других лиц.

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

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

7.2. Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.

7.3. Руководитель, разрешающий доступ сотрудника к конфиденциальному документу, несет персональную ответственность за данное разрешение.

7.4. Каждый сотрудник организации, получающий для работы конфиденциальный документ, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

7.5. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, обучающегося, абитуриента, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

7.5.1. За неисполнение или ненадлежащее исполнение работником по его вине возложенных на него обязанностей по соблюдению установленного порядка работы со сведениями конфиденциального характера работодатель вправе применять предусмотренные Трудовым кодексом дисциплинарные взыскания.

7.5.2. Должностные лица, в обязанность которых входит ведение персональных данных сотрудника, обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом. Неправомерный отказ в предоставлении собранных в установленном порядке документов, либо несвоевременное предоставление таких документов или иной информации в случаях, предусмотренных законом, либо предоставление неполной или заведомо ложной информации - влечет наложение на должностных лиц административного штрафа в размере, определяемом Кодексом об административных правонарушениях.

7.5.3. В соответствии с Гражданским кодексом лица, незаконными методами получившие информацию, составляющую служебную тайну (в том числе персональные данные), обязаны возместить причиненные убытки, причем такая же обязанность возлагается и на обучающегося.

7.5.4. Уголовная ответственность за нарушение неприкосновенности частной жизни (в том числе незаконное собирание или распространение сведений о частной жизни лица, составляющего его личную или семейную тайну, без его согласия), неправомерный доступ к охраняемой законом компьютерной информации, неправомерный отказ в предоставлении собранных в установленном порядке документов и сведений (если эти деяния причинили вред правам и законным интересам граждан), совершенные лицом с использованием своего служебного положения наказывается штрафом, либо лишением права занимать определенные должности или заниматься определенной деятельностью, либо арестом в соответствии с УК РФ.

7.6. Неправомерность деятельности органов государственной власти и организации по сбору и использованию персональных данных может быть установлена в судебном порядке.

Согласовано:

Председатель Студенческого совета — органа студенческого самоуправления

_____ М.З. Газаль

«29» августа 2019