

Министерство культуры Российской Федерации
федеральное государственное бюджетное образовательное учреждение
высшего образования
«ХАБАРОВСКИЙ ГОСУДАРСТВЕННЫЙ
ИНСТИТУТ КУЛЬТУРЫ»
(ХГИК)

ПРИНЯТО

Решением Ученого совета
от «27» января 2016 года, протокол № 5

УТВЕРЖДЕНО

Приказом ФГБОУ ВО
«Хабаровский государственный
институт культуры»

от «20» 06 20 16 г. № 141-06



**ПОЛОЖЕНИЕ
ПО ОБРАБОТКЕ И ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ
СУБЪЕКТОВ**
федерального государственного бюджетного образовательного
учреждения высшего образования «Хабаровский государственный
институт культуры»
(НОВАЯ РЕДАКЦИЯ)

г. Хабаровск
2016 г.

1. Общие положения

1.1. Настоящее Положение разработано в соответствии с законодательством Российской Федерации о персональных данных (далее по тексту - ПДн):
Федеральный закон от 27.07.2006г. № 152-ФЗ «О персональных данных»;
Федеральный закон от 29.12.2012г. N 273-ФЗ «Об образовании в Российской Федерации»;

Трудовой кодекс РФ;

Постановление Правительства РФ от 15.09.08г. N 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

Постановление Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при обработке в информационных системах персональных данных»;

Постановление Правительства РФ от 10.07.2013г. № 582 «Об утверждении Правил размещения на официальном сайте образовательной организации в информационно-телекоммуникационной сети Интернет и обновления информации об образовательной организации».

1.2. В настоящем Положении используются следующие термины:

персональные данные (ПДн) - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту ПДн);

обработка ПДн - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с ПДн, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн;

автоматизированная обработка ПДн - обработка ПДн с помощью средств вычислительной техники;

распространение ПДн - действия, направленные на раскрытие ПДн неопределенному кругу лиц;

предоставление ПДн - действия, направленные на раскрытие ПДн определенному лицу или определенному кругу лиц;

блокирование ПДн - временное прекращение обработки ПДн (за исключением случаев, если обработка необходима для уточнения ПДн);

уничтожение ПДн - действия, в результате которых становится невозможным восстановить содержание ПДн в ИСПДн и /или в результате которых уничтожаются материальные носители ПДн;

обезличивание ПДн - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность ПДн конкретному субъекту ПДн;

информационная система персональных данных (ИСПДн) - совокупность содержащихся в базах данных ПДн и обеспечивающих их обработку информационных технологий и технических средств.

1.3. Настоящее Положение определяет порядок и условия обработки ПДн в федеральном государственном бюджетном образовательном учреждении высшего образования «Хабаровский государственный институт культуры» (далее по тексту - ХГИК), включая порядок передачи ПДн третьим лицам, особенности автоматизированной и неавтоматизированной обработки ПДн, порядок доступа к ПДн, систему защиты ПДн, порядок организации внутреннего контроля и ответственность за нарушения при обработке ПДн, иные вопросы.

1.4. Действие настоящего Положения распространяется на все процессы по сбору, систематизации, накоплению, хранению, уточнению, использованию, распространению (в том числе передаче), обезличиванию, блокированию, уничтожению ПДн, осуществляемых с использованием средств автоматизации и без их использования.

1.5. Настоящее Положение вступает в силу с момента его утверждения и действует бессрочно, до замены его новым Положением.

1.6. Все изменения в Положение вносятся приказом.

2. Цели и задачи обработки ПДн

2.1. Обработка ПДн должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка ПДн, несовместимая с целями сбора ПДн.

2.2. Не допускается объединение баз данных, содержащих ПДн, обработка которых осуществляется в целях, несовместимых между собой.

2.3. Обработке подлежат только ПДн, которые отвечают целям их обработки.

2.4. Содержание и объем, обрабатываемых ПДн, должны соответствовать заявленным целям обработки. Обрабатываемые ПДн не должны быть избыточными по отношению к заявленным целям их обработки.

2.5. Обработка ПДн работников ХГИК может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества ХГИК.

2.6. Основными целями обработки ПДн является:

- осуществление и выполнение функций, полномочий и обязанностей, возложенных на ХГИК законодательством Российской Федерации, Уставом и (или) договором;
- исполнение договора, стороной которого либо выгодоприобретателем по которому является субъект ПДн, а также для заключения договора по инициативе субъекта ПДн или договора, по которому субъект ПДн будет являться выгодоприобретателем.

2.7. Дополнительными целями обработки ПДн являются:

- обеспечение оперативного планирования и управления учебным процессом;

- автоматизация административно-хозяйственной деятельности и управления;
- обеспечение автоматизации бухгалтерского и налогового учета;
- формирование оперативной отчетности;
- автоматизация библиотечных процессов, включая подключение к электронной библиотечной системе.

3. Персональные данные, обрабатываемые в ХГИК

3.1. В ХГИК обрабатываются ПДн следующих субъектов ПДн:

- 3.1.1. работники;
 - 3.1.2. обучающиеся;
 - 3.1.3. абитуриенты;
 - 3.1.4. родители и законные представители обучающихся;
 - 3.1.5. другие физические лица, состоящие в договорных отношениях с ХГИК.
- 3.2. Данный перечень может пересматриваться по мере необходимости.

4. Доступ к ПДн

4.1. Работники ХГИК, которые в силу выполняемых служебных обязанностей постоянно работают с ПДн, получают доступ к необходимым категориям ПДн на срок выполнения ими соответствующих должностных обязанностей. Перечень лиц, допущенных к работе с ПДн, утверждается ректором ХГИК.

4.2. Список лиц, имеющих доступ к ПДн должен поддерживаться в актуальном состоянии.

4.3. В ХГИК установлен разрешительный порядок доступа к ПДн. Работникам ХГИК предоставляется доступ к работе с ПДн исключительно в пределах и объеме, необходимых для выполнения ими своих должностных обязанностей.

4.4. Доступ к ПДн третьих лиц, не являющихся работникам ХГИК без согласия субъекта ПДн, запрещен, за исключением доступа работников органов исполнительной власти, осуществляемого в рамках мероприятий по контролю и надзору за исполнением законодательства, реализации функций и полномочий соответствующих органов государственной власти. Предоставление информации по запросу или требованию органа государственной власти осуществляется с ведома ректора ХГИК.

4.5. В случае если работнику сторонней организации необходим доступ к ПДн, то необходимо, чтобы в договоре со сторонней организацией были прописаны условия конфиденциальности ПДн и обязанность сторонней организации и ее работников по соблюдению требований законодательства в области защиты ПДн. Кроме того, в случае доступа к ПДн лиц, не являющихся работниками ХГИК, должно быть получено согласие субъектов ПДн на предоставление их ПДн третьим лицам. Указанное согласие не требуется, если ПДн предоставляются в целях исполнения гражданско-правового договора, заключенного ХГИК с субъектом ПДн.

4.6. Доступ работника ХГИК к ПДн прекращается с даты, прекращения трудовых отношений, либо даты изменения должностных обязанностей

работника и/или исключения работника из списка лиц, имеющих право доступа к ПДн. В случае увольнения все носители, содержащие ПДн, которые в соответствии с должностными обязанностями находились в распоряжении работника во время работы, должны быть переданы соответствующему должностному лицу.

5. Основные требования по защите ПДн

5.1. При обработке ПДн в информационной системе должно быть обеспечено:

- а) проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и/или передачи их лицам, не имеющим права доступа к такой информации;
- б) своевременное обнаружение фактов несанкционированного доступа к ПДн;
- в) недопущение воздействия на технические средства автоматизированной обработки ПДн, в результате которого может быть нарушено их функционирование;
- г) возможность незамедлительного восстановления ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- д) постоянный контроль над обеспечением уровня защищенности ПДн.

5.2. В ХГИК должны приниматься необходимые правовые, организационные, технические и другие меры для обеспечения безопасности ПДн.

5.3. Для разработки требований по обеспечению безопасности и внедрения системы обеспечения безопасности ПДн разработана "Частная модель угроз безопасности ИСПДн" на основе нормативно-методического документа ФСТЭК России «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных».

5.4. В ХГИК в соответствии с руководящими документами государственных органов власти осуществлена классификация ИСПДн, о чем Комиссией ХГИК составлены Акты классификации ИСПДн.

5.5. В ХГИК на основании Акта проверки ИСПДн и в соответствии с нормативно-методическим документом ФСТЭК России «Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных» разработан и внедряется комплекс мер по защите и обеспечению безопасности ПДн.

5.6. В ХГИК используются технические средства и программное оборудование для обработки и защиты ПДн.

5.7. Все лица, допущенные к работе с ПДн, а также связанные с эксплуатацией и техническим сопровождением ИСПДн должны быть ознакомлены с требованиями настоящего Положения и другими нормативными документами ХГИК в области обработки и защиты ПДн.

5.8. В ХГИК организован процесс обучения использования средств защиты ПДн. Обучение по данному направлению рекомендовано лицам, имеющим постоянный доступ к ПДн, и лицам, эксплуатирующим технические и программные средства ИСПДн и средства защиты ИСПДн.

5.9. Работники обязаны незамедлительно сообщать руководителю ХГИК, ответственному за организацию обработки ПДн об утрате или недостатке носителей информации, содержащих ПДн, а также о причинах и условиях возможной утечки ПДн.

5.10. В случае попытки посторонних лиц получить от работника ХГИК персональные данные, обрабатываемых в ХГИК, работник должен незамедлительно известить об этом соответствующее должностное лицо ХГИК.

6. Согласие на обработку ПДн

6.1. Субъект ПДн принимает решение о предоставлении ПДн и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку ПДн должно быть конкретным и сознательным. Согласие на обработку ПДн может быть дано субъектом ПДн или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено законодательством РФ. В случае получения согласия на обработку ПДн от представителя субъекта ПДн полномочия данного представителя на дачу согласия от имени субъекта ПДн должно быть проверено.

6.2. Получение письменного согласия на обработку ПДн осуществляется работником ХГИК, при получении ПДн от субъекта ПДн, путем оформления письменного согласия (Приложение 1,2,3,4,5,6), а также разъяснения о последствиях отказа в предоставлении ПДн (Приложения 7,8).

7. Права субъекта в отношении ПДн

7.1. Субъект ПДн имеет право:

- на получение информации, касающейся обработки его ПДн. Сведения должны быть предоставлены субъекту ПДн в доступной форме, и в них не должны содержаться ПДн, относящиеся к другим субъектам ПДн, за исключением случаев, если имеются законные основания для раскрытия таких ПДн. Перечень сведений и порядок получения сведений предусмотрен действующим законодательством РФ;
- требовать уточнения его ПДн, 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 законодательством РФ меры по защите своих прав;
- на условие предварительного письменного согласия при обработке ПДн в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи, а также в целях политической агитации;
- на условие письменного согласия при принятии на основании исключительно автоматизированной обработки ПДн решений, порождающих юридические последствия в отношении субъекта ПДн или иным образом затрагивающих его права и законные интересы;
- заявлять возражения на решения, основанные на автоматизированной обработке его ПДн и возможные юридические последствия такого решения;

- обжаловать действия или бездействие работников ХГИК в уполномоченный орган по защите прав субъектов ПДн или в судебном порядке.

8. Права и обязанности ХГИК

8.1. ХГИК вправе:

8.1.1. Поручить обработку ПДн другому лицу с согласия субъекта ПДн, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия государственным или муниципальным органом соответствующего акта.

8.1.2. В случае отзыва субъектом ПДн согласия на обработку ПДн, продолжить обработку ПДн без согласия субъекта ПДн при наличии оснований, указанных в законодательстве РФ.

8.1.3. Отказать субъекту ПДн в выполнении повторного запроса сведений, не соответствующего условиям, предусмотренным законодательством РФ. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на ХГИК.

8.1.4. Самостоятельно определять состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных законодательством РФ.

8.2. ХГИК обязан:

8.2.1. До начала обработки ПДн обязан уведомить уполномоченный орган по защите прав субъектов ПДн о своем намерении осуществлять обработку ПДн, за исключением случаев, предусмотренных законодательством РФ.

8.2.2. При получении доступа к ПДн не раскрывать третьим лицам и не распространять ПДн без согласия субъекта ПДн, если иное не предусмотрено федеральным законом.

8.2.3. Представить доказательство получения согласия субъекта ПДн на обработку его ПДн или доказательство наличия законных оснований, обработки ПДн без согласия субъекта ПДн.

8.2.4. При сборе ПДн, предоставить субъекту ПДн по его просьбе информацию, предусмотренную законодательством РФ.

Если предоставление ПДн для субъекта ПДн является обязательным в соответствии с федеральным законом, ХГИК обязан разъяснить субъекту ПДн юридические последствия отказа предоставить его ПДн.

8.2.5. Если ПДн получены не от субъекта ПДн, ХГИК, за исключением случаев, предусмотренных законодательством РФ, до начала обработки таких ПДн, должен предоставить субъекту ПДн следующую информацию:

- 1) цель обработки ПДн и ее правовое основание;
- 2) предполагаемые пользователи ПДн;
- 3) установленные настоящим Федеральным законом права субъекта ПДн;
- 4) источник получения ПДн.

8.2.6. Опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему политику ХГИК в отношении обработки ПДн, к сведениям о реализуемых требованиях к защите ПДн.

8.2.7. При обработке ПДн принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн.

8.2.8. Сообщить в порядке, предусмотренном законодательством РФ, субъекту ПДн или его представителю информацию безвозмездно о наличии ПДн, относящихся к соответствующему субъекту ПДн, а также предоставить возможность ознакомления с этими ПДн при обращении субъекта ПДн или его представителя либо в течение тридцати дней с даты получения запроса субъекта ПДн или его представителя.

8.2.9. В случае отказа в предоставлении информации о наличии ПДн о соответствующем субъекте ПДн или ПДн субъекту ПДн или его представителю при их обращении либо при получении запроса субъекта ПДн или его представителя ХГИК обязан дать в письменной форме мотивированный ответ, содержащий ссылку на положение законодательства РФ, являющееся основанием для такого отказа, в срок, не превышающий тридцати дней со дня обращения субъекта ПДн или его представителя либо с даты получения запроса субъекта ПДн или его представителя.

8.2.10. В срок, не превышающий семи рабочих дней со дня предоставления субъектом ПДн или его представителем сведений, подтверждающих, что ПДн являются неполными, неточными или неактуальными, ХГИК обязан внести в них необходимые изменения. В срок, не превышающий семи рабочих дней со дня представления субъектом ПДн или его представителем сведений, подтверждающих, что такие ПДн являются незаконно полученными или не являются необходимыми для заявленной цели обработки, ХГИК обязан уничтожить такие ПДн. ХГИК обязан уведомить субъекта ПДн или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым ПДн этого субъекта были переданы.

8.2.11. Сообщить в уполномоченный орган по защите прав субъектов ПДн по запросу этого органа необходимую информацию в течение тридцати дней с даты получения такого запроса.

8.2.12. В случае выявления неправомерной обработки ПДн, осуществляемой ХГИК или лицом, действующим по поручению ХГИК, ХГИК в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку ПДн или обеспечить прекращение неправомерной обработки ПДн лицом, действующим по поручению ХГИК. В случае если обеспечить правомерность обработки ПДн невозможно, ХГИК в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки ПДн, обязан уничтожить такие ПДн или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении

ПДн ХГИК обязан уведомить субъекта ПДн или его представителя, а в случае, если обращение субъекта ПДн или его представителя либо запрос уполномоченного органа по защите прав субъектов ПДн были направлены уполномоченным органом по защите прав субъектов ПДн, также указанный орган.

8.2.13. В случае отзыва субъектом ПДн согласия на обработку его ПДн, прекратить их обработку или обеспечить прекращение такой обработки (если обработка ПДн осуществляется другим лицом, действующим по поручению ХГИК) и в случае, если сохранение ПДн более не требуется для целей обработки ПДн, уничтожить ПДн или обеспечить их уничтожение (если обработка ПДн осуществляется другим лицом, действующим по поручению ХГИК) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, иным соглашением между ХГИК и субъектом ПДн либо если ХГИК не вправе осуществлять обработку ПДн без согласия субъекта ПДн на основаниях, предусмотренных законодательством РФ.

8.2.14. Назначить лицо, ответственное за организацию обработки ПДн.

9. Порядок обработки и защиты ПДн

9.1. Обеспечение конфиденциальности ПДн, обрабатываемых в ХГИК, является обязательным требованием для всех лиц, которым ПДн стали известны.

9.2. Работники ХГИК, осуществляющие оформление документов, обязаны получать в установленных случаях согласие субъектов ПДн на обработку.

9.3. В случае нарушения установленного порядка обработки ПДн работники ХГИК несут ответственность в соответствии с разделом 11 настоящего Положения.

9.4. Помещения ХГИК, по окончании рабочего дня и отсутствия работников в помещениях, должны запираются, окна должны быть закрыты, должна быть включена сигнализация (при наличии).

9.5. Сетевое оборудование, серверы следует располагать в местах, недоступных для посторонних лиц (в специальных помещениях, шкафах, коробах).

9.6. Уборка помещений и обслуживание технических средств ИСПДн должна осуществляться под контролем ответственных за данные помещения и технические средства лиц с соблюдением мер, исключающих несанкционированный доступ к ПДн, носителям информации, программным и техническим средствам обработки, передачи и защиты информации ИСПДн.

9.7. Порядок обработки и защиты ПДн, обрабатываемых без использования средств автоматизации изложен в Инструкции по обработке персональных данных без использования средств автоматизации.

9.8. Порядок обработки и защиты ПДн, обрабатываемых в ИСПДн изложен в Инструкции пользователя ИСПДн.

9.9. Организация внутреннего контроля процесса обработки ПДн в ХГИК осуществляется в целях изучения и оценки фактического состояния защищенности ПДн, своевременного реагирования на нарушения установленного порядка их обработки, а также в целях совершенствования этого порядка и обеспечения его соблюдения.

9.10. Мероприятия по осуществлению внутреннего контроля обработки и обеспечения безопасности ПДн направлены на решение следующих задач:

9.10.1. Обеспечение соблюдения работниками ХГИК требований настоящего Положения и нормативно-правовых актов, регулирующих сферу ПДн.

9.10.2. Оценка компетентности персонала, задействованного в обработке ПДн.

9.10.3. Обеспечение работоспособности и эффективности технических средств ИСПДн и средств защиты ПДн, их соответствия требованиям уполномоченных органов исполнительной власти по вопросам безопасности ПДн.

9.10.4. Выявление нарушений установленного порядка обработки ПДн и своевременное предотвращение негативных последствий таких нарушений.

9.10.5. Принятие корректирующих мер, направленных на устранение выявленных нарушений, как в порядке обработки ПДн, так и в работе технических средств ИСПДн.

9.10.6. Разработка рекомендаций по совершенствованию порядка обработки и обеспечения безопасности ПДн по результатам контрольных мероприятий.

9.10.7. Осуществление внутреннего контроля за исполнением рекомендаций и указаний по устранению нарушений.

9.11. Результаты контрольных мероприятий оформляются актами и являются основанием для разработки рекомендаций по совершенствованию порядка обработки и обеспечения безопасности ПДн, по модернизации технических средств ИСПДн и средств защиты ПДн, по обучению и повышению компетентности персонала, задействованного в обработке ПДн.

10. Особенности управления ПДн работников ХГИК

10.1. В настоящем разделе установлены дополнительные права и обязанности ХГИК и работников при обработке ПДн работников ХГИК.

10.2. ПДн работника - информация, необходимая ХГИК в связи с трудовыми отношениями и касающаяся конкретного работника.

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

10.4. ХГИК не имеет права получать и обрабатывать ПДн работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральными законами.

10.5. При принятии решений, затрагивающих интересы работника, ХГИК не имеет права основываться на ПДн работника, полученных исключительно в результате их автоматизированной обработки или электронного получения.

10.6. Работники не должны отказываться от своих прав на сохранение и защиту тайны.

10.7. ХГИК обязуется не сообщать ПДн работника в коммерческих целях без его письменного согласия.

10.8. ХГИК обязуется предупредить работников ХГИК, третьих лиц, получающих ПДн работника (при его согласии), 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 ПДн работника, обязаны соблюдать режим секретности (конфиденциальности).

10.9. Доступ к ПДн работников осуществляется на основании приказов и положений, утвержденных ректором ХГИК.

10.10. Работник имеет право на определение своих представителей для защиты своих ПДн.

11. Ответственность за нарушение настоящего положения

11.1. Руководство ХГИК несет ответственность за необеспечение конфиденциальности ПДн и несоблюдение прав и свобод субъектов ПДн в отношении их ПДн, в том числе прав на неприкосновенность частной жизни, личную и семейную тайну.

11.2. Работники ХГИК несут персональную ответственность за несоблюдение требований по обработке и обеспечению безопасности ПДн, установленных настоящим Положением и Инструкциями по обработке персональных данных, в соответствии с законодательством Российской Федерации.

11.3. Работник ХГИК может быть привлечен к ответственности в случаях:

11.3.1. Умышленного или неосторожного раскрытия ПДн;

11.3.2. Утраты материальных носителей ПДн;

11.3.3. Нарушения требований настоящего Положения и других нормативных документов ХГИК в части вопросов доступа и работы с ПДн.