БЕЛОЯРСКИЙ РАЙОН

ХАНТЫ-МАНСИЙСКИЙ АВТОНОМНЫЙ ОКРУГ - ЮГРА

ИНДИВИДУАЛЬНЫЙ ПРЕДПРИНИМАТЕЛЬ

АКСЕНОВ ТИМОФЕЙ СЕРГЕЕВИЧ

Г. БЕЛОЯРСКИЙ, 3 МКР, 13, 32

ТЕЛЕФОН: +7(922)2049227

ИНН: 666203578748

УТВЕРЖДАЮ
ИП Аксенов Тимофей Сергеевич

«20» февраля 2015 г.

ПОЛИТИКА
конфиденциальности и порядок обработки персональных данных при подаче заявок в ИП Аксенов Тимофей Сергеевич

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Политика разработана в соответствии с Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Указом Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера», Постановлением Правительства РФ от 17.11.2007 № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», постановлением Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», иными нормативными правовыми актами Российской Федерации, Уставом ГОУ ВПО «БГУ», иными локальными нормативными документами муниципального автономного учреждении культуры Белоярского района «Белоярской ЦБС» (далее - Организация).

1.2. Настоящая Политика устанавливает в Организации порядок работы с документами – носителями информации, содержащей персональные данные, в целях:

– предотвращения неконтролируемого распространения информации, содержащей персональные данные в результате ее разглашения должностным лицом, имеющим доступ к информации, содержащей персональные данные, или получения несанкционированного доступа к информации;

– предотвращения несанкционированного уничтожения, искажения, копирования, блокирования информации, содержащей персональные данные;

– предотвращения утраты, несанкционированного уничтожения или сбоев в процессе функционирования автоматизированных систем обработки информации, содержащей персональные данные, обеспечение полноты, целостности, достоверности такой информации;

– соблюдения правового режима использования информации, содержащей персональные данные;

– обеспечения возможности обработки и использования персональных данных Организацией и должностными лицами, имеющими соответствующие полномочия.

1.3. Обработка персональных данных осуществляется Организацией с согласия субъекта персональных данных.

Согласие субъекта на обработку его персональных данных не требуется в следующих случаях:

- если персональные данные являются общедоступными;
- когда персональные данные относятся к состоянию здоровья работника и их обработка необходима для защиты его жизни, здоровья или иных жизненно важных интересов либо жизни, здоровья или иных жизненно важных интересов других лиц, а получение согласия работника невозможно;
- если обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;
- обработки персональных данных по требованию уполномоченных на то государственных органов в случаях, предусмотренных федеральным законом;
- когда обработка персональных данных осуществляется в целях исполнения обращения, запроса самого субъекта персональных данных, трудового или иного договора с ним;
- обработки адресных данных, необходимых для доставки почтовых отправлений организациями почтовой связи;
- обработки данных, включающих в себя только фамилии, имена и отчества;
- когда обработка персональных данных осуществляется в целях однократного пропуска на территорию Организации или в иных аналогичных целях;
- обработки персональных данных без использования средств автоматизации.

1.4. В целях обеспечения сохранности и конфиденциальности информации, содержащей персональные данные, все операции по оформлению, формированию, ведению и хранению данной информации должны выполняться специалистами Организации, осуществляющими данную работу в соответствии со своими служебными обязанностями, зафиксированными в их должностных Политиках.

1.5. Режим конфиденциальности персональных данных отменяется в случаях обезличивания этих данных, в отношении персональных данных, ставших общедоступными, или по истечении 75-летнего срока их хранения, если иное не предусмотрено законом.

1.6. В структурных подразделениях Организации, имеющих доступ к информации, содержащей персональные данные, формируются и ведутся перечни персональных данных с указанием регламентирующих документов, мест хранения и лиц, ответственных за хранение и обработку данных.

Осуществлять обработку и хранение данных, в местах не внесенных в перечень, не допускается.

2. ПОРЯДОК ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПРИ ОБРАБОТКЕ И ХРАНЕНИИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОСУЩЕСТВЛЯЕМЫХ С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ АВТОМАТИЗАЦИИ

2.1. Безопасность персональных данных при их обработке в автоматизированных информационных системах обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации, а также используемые в информационной системе информационные технологии.

2.2. Допуск должностных лиц к обработке персональных данных в автоматизированной информационной системе осуществляется на основании соответствующих разрешительных документов и ключей доступа (паролей).

2.3. Размещение автоматизированных информационных систем, специальное оборудование и организация с их использованием работы с персональными данными должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого пребывания в соответствующих помещениях посторонних лиц.

2.4. Компьютеры и(или) электронные папки, в которых содержатся файлы с персональными данными, для каждого пользователя должны быть защищены индивидуальными паролями доступа, состоящими из 6 и более символов. Работа на компьютерах с персональными данными без паролей доступа или под чужими, а равно общими (одинаковыми) паролями, не допускается.

2.5. Пересылка персональных данных без использования специальных средств защиты по общедоступным сетям связи, в том числе Интернет, не допускается.

2.6. Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

2.7. При обработке персональных данных в информационной системе пользователями должно быть обеспечено:

– использование предназначенных для этого разделов (каталогов) носителей информации, встроенных в технические средства, или съемных маркированных носителей;

– недопущение физического воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

– постоянное использование антивирусного обеспечения для обнаружения зараженных файлов и незамедлительное восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

– недопущение несанкционированных выноса из помещений, установки, подключения оборудования, а также удаления, инсталляции или настройки программного обеспечения.

2.8. При обработке персональных данных в автоматизированной информационной системе разработчиками и администраторами систем должны обеспечиваться:

– обучение лиц, использующих средства защиты информации, применяемые в автоматизированных информационных системах, правилами работы с ними;

– учет лиц, допущенных к работе с персональными данными в автоматизированной информационной системе, прав и паролей доступа;

– учет применяемых средств защиты информации, эксплуатационной и технической документации к ним;

– контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

– описание системы защиты персональных данных;

– иные требования по защите персональных данных, установленных Политиками Организации по их использованию и эксплуатации.

2.9. Особенности обеспечения безопасности информации и персональных данных, связанные с использованием конкретных автоматизированных информационных систем, определяются локальными нормативными документами Организации, регламентирующими порядок использования указанных информационных систем, а также эксплуатационной и инструктивной документацией, касающейся технических средств обработки персональных данных в рамках конкретной автоматизированной информационной системы.

3. ПОРЯДОК УЧЕТА, ХРАНЕНИЯ И ОБРАЩЕНИЯ СО СЪЕМНЫМИ НОСИТЕЛЯМИ ПЕРСОНАЛЬНЫХ ДАННЫХ (ИХ ТВЕРДЫМИ КОПИЯМИ), А ТАКЖЕ ИХ УТИЛИЗАЦИИ

3.1 Все находящиеся на хранении и в обращении съемные носители с персональными данными подлежат учёту. Каждый съемный носитель с записанными на нем персональными данными должен иметь этикетку, на которой указывается его уникальный учетный номер.

3.2 Учет и выдачу съемных носителей персональных данных по утвержденной форме осуществляют работники структурных подразделений, на которых возложены функции хранения носителей персональных данных. Работники Организации получают учтенный съемный носитель персональных данных от уполномоченного лица для выполнения работ на конкретный срок. При получении делаются соответствующие записи в журнале учета. По окончании работ пользователь сдает съемный носитель для хранения уполномоченному должностному лицу, о чем делается соответствующая запись в журнале учета.

3.3 Не допускается:

хранение съемных носителей с персональными данными вместе с носителями открытой информации, на рабочих столах, либо оставление их без присмотра или передача на хранение другим лицам;

вынос съемных носителей с персональными данными из служебных помещений для работы с

ними на дому, в гостиницах и т. д.

3.4 При отправке или передаче персональных данных адресатам на съемные носители записываются только предназначенные адресатам данные. Отправка персональных данных адресатам на съемных носителях осуществляется в порядке, установленном для документов имеющих гриф «ДСП» (для служебного пользования). Вынос съемных носителей персональных данных для непосредственной передачи адресату осуществляется только с письменного разрешения руководителя соответствующего структурного подразделения Организации.

3.5 О фактах утраты съемных носителей, содержащих персональные данные, либо разглашения содержащихся на них сведений немедленно ставится в известность руководитель соответствующего структурного подразделения Организации.

На утраченные носители составляется акт. Соответствующие отметки вносятся в журналы учета съемных носителей персональных данных.

3.6 Съемные носители персональных данных, пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению. Уничтожение съемных носителей с информацией осуществляется соответствующей комиссией, состав которой утверждается приказом руководителя Организации. По результатам уничтожения носителей составляется акт утвержденной формы.

3.7 При осуществлении обработки персональных данных с использованием средств автоматизации для каждой информационной системы персональных данных должен быть назначен администратор, а для систем высоких классов – также администратор системы безопасности. Техническое обслуживание оборудования должно осуществляться соответствующим обслуживающим персоналом.

Руководитель организации:

ИП Аксенов Тимофей Сергеевич "20" февраля 2015 г.

(должность) (ФИО) (подпись) (М.П.)