СОГЛАСОВАНО

Уполномоченный представитель
работников МУК «ИЦКЦ»
_____ С.В. Климцева
19 августа 2022 год
(приказ № 134-од от 24.03.2022 года)

УТВЕРЖДАЮ

Директор МУК «ИЦКЦ»
_____ И.В. Бабушкина
19 августа 2022 год
(приказ № 299 – од от 19.08.22 г.)

ПОЛОЖЕНИЕ № 06
О защите персональных данных работников Муниципального учреждения культуры городского округа «Город Архангельск» «Исакогорско-Цигломенский культурный центр

1. Общие положения

1.1. Положение о защите персональных данных муниципального учреждения культуры городского округа «Город Архангельск» «Исакогорско-Цигломенский культурный центр» (далее – Работодатель) разработано в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ и иными нормативно-правовыми актами в области защиты персональных данных, действующими на территории России.

1.2. Цель настоящего Положения – защита персональных данных работников МУК «ИЦКЦ» от несанкционированного доступа и разглашения, предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений.

1.3. В целях настоящего Положения:

- под персональными данными понимается любая информация, прямо или косвенно относящаяся к субъекту персональных данных;
- под угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных;
- под уровнем защищенности персональных данных понимается комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационной системе.

1.4. Настоящее Положение и изменения к нему утверждаются директором МУК «ИЦКЦ», уполномоченным представителем работников и вводятся приказом. Все работники должны быть ознакомлены под подпись с данным Положением и изменениями к нему.

1.5. Настоящее Положение вступает в силу с 01.09.2022.

2. Защита персональных данных

2.1. Работодатель принимает следующие меры по защите персональных данных:

2.1.1. Назначение лица, ответственного за обработку персональных данных, которое осуществляет организацию обработки персональных данных, обучение и инструктаж, внутренний контроль за соблюдением работниками требований к защите персональных данных.

2.1.2. Разработка политики в отношении обработки персональных данных.

2.1.3. Установление правил доступа к персональным данным, обеспечение регистрации и учета всех действий, совершаемых с персональными данными.

2.1.4. Установление индивидуальных паролей доступа сотрудников в информационную систему в соответствии с их производственными обязанностями.

2.1.5. Применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации.

2.1.6. Сертифицированное антивирусное программное обеспечение с регулярно обновляемыми базами.

2.1.7. Соблюдение условий, обеспечивающих сохранность персональных данных и исключающих несанкционированный к ним доступ.

2.1.8. Обнаружение фактов несанкционированного доступа к персональным данным.

2.1.9. Восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

2.1.10. Обучение работников, непосредственно осуществляющих обработку персональных данных, положениям законодательства Российской Федерации о персональных данных, в том числе требованиям к защите персональных данных, документам, определяющим политику Работодателя в отношении обработки персональных данных, локальным актам по вопросам обработки персональных данных.

2.1.11. Осуществление внутреннего контроля и аудита.

2.1.12. Определение типа угроз безопасности и уровней защищенности персональных данных, которые хранятся в информационных системах.

2.2. Угрозы защищенности персональных данных.

2.2.1. Угрозы первого типа. В системном программном обеспечении информационной системы есть функциональные возможности программного обеспечения, которые не указаны в описании к нему либо не отвечают характеристикам, которые заявил производитель. И это потенциально может привести к неправомерному использованию персональных данных.

2.2.2. Угрозы второго типа. Потенциальные проблемы с прикладным программным обеспечением - внешними программами, которые установлены на компьютерах работников.

2.2.3. Угрозы третьего типа. Потенциальной опасности ни от системного, ни от программного обеспечения нет.

2.3. Уровни защищенности персональных данных.

2.3.1. Первый уровень защищенности. Если работодатель отнес информационную систему к первому типу угрозы или если тип угрозы второй, но работодатель обрабатывает специальные категории персональных данных более 100 тыс. физических лиц без учета работников.

2.3.2. Второй уровень защищенности. Если тип угрозы второй и работодатель обрабатывает специальные категории персональных данных работников вне зависимости от их количества или специальные категории персональных данных менее чем 100 тыс. физических лиц, или любые другие категории персональных данных более чем 100 тыс. физических лиц, или при третьем типе угрозы работодатель обрабатывает специальные категории данных более чем 100 тыс. физических лиц.

2.3.3. Третий уровень защищенности. Если при втором типе угрозы работодатель обрабатывает общие персональных данных работников или менее чем 100 тыс. физических лиц, или при третьем типе угрозы работодатель обрабатывает специальные категории персональных данных работников или менее чем 100 тыс. физических лиц, или при третьем типе угрозы работодатель обрабатывает биометрические персональных данных, или при третьем типе угрозы работодатель обрабатывает общие персональных данных более чем 100 тыс. физических лиц.

2.3.4. Четвертый уровень защищенности. Если при третьем типе угрозы работодатель обрабатывает только общие персональных данных работников или менее чем 100 тыс. физических лиц.

2.4. При четвертом уровне защищенности персональных данных работодатель:

- обеспечивает режим безопасности помещений, в которых размещаете информационную систему;
- обеспечивает сохранность носителей информации;
- утверждает перечень работников, допущенных до персональных данных;

использует средства защиты информации, которые прошли оценку соответствия требованиям закона в области обеспечения безопасности информации.

2.5. При третьем уровне защищенности персональных данных дополнительно к мерам, перечисленным в пункте 2.4. настоящего Положения, работодатель назначает ответственного за обеспечение безопасности персональных данных в информационной системе.

2.6. При втором уровне защищенности персональных данных дополнительно к мерам, перечисленным в пунктах 2.4, 2.5 настоящего Положения, Работодатель ограничивает доступ к электронному журналу сообщений, за исключением работников, которым такие сведения необходимы для работы.

.2.7. При первом уровне защищенности персональных данных дополнительно к мерам, перечисленным в пунктах 2.4-2.6 настоящего Положения, работодатель:

- обеспечивает автоматическую регистрацию в электронном журнале безопасности изменения полномочий работников по допуску к персональных данных в системе;
- создает отдел, ответственный за безопасность персональных данных в системе, либо возлагает такую обязанность на один из существующих отделов работодателя.

2.8. В целях защиты персональных данных на бумажных носителях работодатель:

- приказом назначает ответственного за обработку персональных данных;
- ограничивает допуск в помещения, где хранятся документы, которые содержат персональных данных работников;
- хранит документы, содержащие персональных данных работников в шкафах, запирающихся на ключ;
- хранит трудовые книжки работников в сейфе специалиста (по кадрам).

2.9. В целях обеспечения конфиденциальности документы, содержащие персональных данных работников, оформляются, ведутся и хранятся только у специалистов (по кадрам, специалиста по финансовому и экономическому контролю).

2.10. Специалисты (по кадрам, делопроизводитель, по финансово-экономическому контролю, учету и движению денежных средств), допущенные к персональным данным работников, подписывают обязательства о неразглашении персональных данных. В противном случае до обработки персональных данных работников не допускаются.

2.11. Допуск к документам, содержащим персональных данных работников, внутри организации осуществляется на основании Регламента допуска работников к обработке персональных данных.

2.12. Передача персональных данных по запросам третьих лиц, если такая передача прямо не предусмотрена законодательством Российской Федерации, допускается исключительно с согласия работника на обработку его персональных данных в части их предоставления или согласия на распространение персональных данных.

2.13. Передача информации, содержащей сведения о персональных данных работников, по телефону в связи с невозможностью идентификации лица, запрашивающего информацию, запрещается.

3. Гарантии конфиденциальности персональных данных

3.1. Все работники организации, осуществляющие обработку персональных данных, обязаны хранить тайну о сведениях, содержащих персональных данных, в соответствии с Положением, требованиями законодательства Российской Федерации.

3.2. Работник вправе требовать полную информацию о своих персональных данных, об их обработке, использовании и хранении.

3.3. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работников, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством.

Литвинова С.В.

СОГЛАСИЕ
НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ

Я,

_____,

(Ф.И.О.)

Проживающий по адресу:

_____

Паспорт серия _____ №_____,
выданный_____

_____

_____

(кем и когда)

даю свое согласие на обработку в **Муниципальное учреждение культуры городского округа «Город Архангельск» «Исакогорско-Цигломенский культурный центр» (далее – МУК «ИЦКЦ»)** моих персональных данных, относящихся исключительно к перечисленным ниже категориям персональных данных:

- паспортные данные;
- данные страхового Свидетельства государственного пенсионного страхования (СНИЛС);
- данные документа воинского учета[1];
- документы об образовании, профессиональной переподготовке, повышении квалификации, стажировки, присвоении ученой степени, ученого звания (если таковые имеются);
- анкетные данные, предоставленные мною при поступлении на работу или в процессе работы (в том числе - автобиография, сведения о семейном положении работника, перемене фамилии, наличии детей и иждивенцев);
- данные иных документов, которые с учетом специфики работы и в соответствии с законодательством Российской Федерации должны быть предъявлены мною при заключении трудового договора или в период его действия[2];
- справка о наличии (отсутствии) судимости и (или) факта уголовного преследования либо о прекращении уголовного преследования;
- данные трудового договора и соглашений к нему;
- данные кадровых приказов о моем приеме, переводах, увольнении;
- данные личной карточки по формам Т-2;
- данные документов о прохождении мной аттестации, собеседования, повышения квалификации, результатов оценки и обучения;
- фотография;

– иные сведения обо мне, которые необходимо МУК «ИЦКЦ» для корректного документального оформления правоотношений между мною и МУК «ИЦКЦ».

Я даю согласие на использование персональных данных исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, получении образования и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

Настоящее согласие предоставляется мной на осуществление действий в отношении моих персональных данных, которые необходимы для достижения указанных выше целей, включая (без ограничения) сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, передачу третьим лицам для осуществления действий по обмену информацией, обезличивание, блокирование персональных данных, а также осуществление любых иных действий, предусмотренных действующим законодательством Российской Федерации.

Я проинформирован, что МУК «ИЦКЦ» гарантирует обработку моих персональных данных в соответствии с действующим законодательством Российской Федерации как неавтоматизированным, так и автоматизированным способами.

Данное согласие действует до достижения целей обработки персональных данных или в течение срока хранения информации.

Данное согласие может быть отозвано в любой момент по моему письменному заявлению.

Я подтверждаю, что, давая такое согласие, я действую по собственной воле и в своих интересах.

«____» _____ 20__ г. _____ _____

(подпись) (расшифровка подписи)

[1] Только для военнообязанных и лиц, подлежащих призыву на военную службу.

[2] Например, медицинские заключения, при прохождении обязательных предварительных и периодических медицинских осмотров и т.д.

СОГЛАСИЕ
НА РАЗМЕЩЕНИЕ ФОТОГРАФИЙ, ЛИЧНОЙ ИНФОРМАЦИИ

Я,

_____,
(Ф.И.О.)

Паспорт серия _____ №_____,

выданный_____

_____

(кем и когда)

настоящим даю / не даю (нужное подчеркнуть) свое согласие Оператору МУК «ИЦКЦ» на размещение фотографий, личной информации (ФИО, должность, дата рождения):

В социальной сети «В контакте» по адресам:
- https://vk.com/ickc_29
- https://vk.com/bakariza29
-https://vk.com/isakogorka29,
- https://vk.com/turdeevo29

с целью: поздравления работника с личными праздниками (день рождения, награды, свадьба, рождение ребёнка и пр.) и т.д.

В СМИ с целью: опубликования мероприятий, фестивалей и конкурсов.

По первому требованию сотрудника согласие отзывается письменным заявлением.

Данное согласие действует с «___» _____ 20___ года на период действия трудового договора с МУК «ИЦКЦ».

«____» _____ 20__ г. _____ _____
(подпись) (расшифровка подписи)

ОБЯЗАТЕЛЬСТВО
О НЕРАЗГЛАШЕНИИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Я, _____,
(Ф.И.О.)
Паспорт серия _____ №_____,
выданный_____
_____
(кем и когда)

понимаю, что получаю доступ к персональным данным работников МУК «ИЦКЦ». Я также понимаю, что во время исполнения своих обязанностей я занимаюсь сбором, обработкой и хранением персональных данных работников.

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

В связи с этим даю обязательство при работе (сборе, обработке и хранении) с персональными данными сотрудника соблюдать все описанные в Положении о персональных данных требования.

Я подтверждаю, что не имею права разглашать сведения о перечисленных ниже категориях персональных данных:

- паспортные данные;
- данные страхового Свидетельства государственного пенсионного страхования (СНИЛС);
- данные документа воинского учета (для военнообязанных);
- документы об образовании, профессиональной переподготовке, повышении квалификации, стажировки, присвоении ученой степени, ученого звания (если таковые имеются);
- анкетные данные, предоставленные при поступлении на работу или в процессе работы (в том числе - автобиография, сведения о семейном положении работника, перемене фамилии, наличии детей и иждивенцев);
-данные иных документов, которые с учетом специфики работы и в соответствии с законодательством Российской Федерации должны быть предъявлены при заключении трудового договора или в период его действия;
- справка о наличии (отсутствии) судимости и (или) факта уголовного преследования либо о прекращении уголовного преследования;
- данные трудового договора и соглашений к нему;
- данные кадровых приказов о моем приеме, переводах, увольнении;
- данные личной карточки по формам Т-2;
- данные документов о прохождении аттестации, собеседования, повышения квалификации, результатов оценки и обучения;
- фотография;

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

С Положением о порядке обработки персональных данных работников МУК «ИЦКЦ» и гарантиях их защиты ознакомлен(а).

_____ _____ _____
(должность) (подпись) (расшифровка подписи)

«____» _____ 20__ г.

СОГЛАСИЕ НА ПЕРЕДАЧУ ПЕРСОНАЛЬНЫХ ДАННЫХ ТРЕТЬЕЙ СТОРОНЕ

Я_____,
(ФИО)

паспорт_____ выдан _____
(серия, номер)

_____,
(когда и кем выдан)

Адрес регистрации _____

_____,

в целях начисления мне заработной платы, ведения бухгалтерского и налогового учета даю согласие Муниципальное учреждение культуры городского округа «Город Архангельск» «Исакогорско-Цигломенский культурный центр», расположенного по адресу г. Архангельск, ул. Севстрой, д.2 на автоматизированную, а также без использования средств автоматизации обработку моих персональных данных, а именно на предоставление персональных данных муниципальному казенному учреждению «Центр бухгалтерского и экономического обслуживания».

Перечень моих персональных данных, на обработку которых я даю согласие:

- фамилия, имя, отчество;
- пол, возраст;
- дата и место рождения;
- паспортные данные;
- СНИЛС
- банковские реквизиты
- ИНН
- свидетельство о рождении детей
- справка формы 2НДФЛ
- справка формы 182н

Настоящее согласие действует со дня его подписания до дня отзыва в письменной форме.

«____» _____ 20__ г. _____ _____
(подпись) (расшифровка подписи)