

ДЕПАРТАМЕНТ КУЛЬТУРЫ ГОРОДА МОСКВЫ  
ПРЕФЕКТУРА СЕВЕРО-ЗАПАДНОГО АДМИНИСТРАТИВНОГО ОКРУГА ГОРОДА МОСКВЫ  
**ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ ГОРОДА МОСКВЫ  
«ОБЪЕДИНЕНИЕ КУЛЬТУРНЫХ И ДОСУГОВЫХ ЦЕНТРОВ  
СЕВЕРО-ЗАПАДНОГО АДМИНИСТРАТИВНОГО ОКРУГА»**

**П Р И К А З**

22 сентября 2025 г.

№ 06-88-6

**Об утверждении Положения по организации и проведению работ  
по обеспечению безопасности персональных данных при их обработке  
в Государственном бюджетном учреждении города Москвы  
«Объединение культурных и досуговых центров  
Северо-Западного административного округа»**

В связи с переименованием 22.09.2025 Государственного бюджетного учреждения города Москвы «Крылья» в Государственное бюджетное учреждение города Москвы «Объединение культурных и досуговых центров Северо-Западного административного округа» (п. 1 совместного приказа Департамента культуры города Москвы и префектуры Северо-Западного административного округа города Москвы от 16.09.2025 № 91/837/ОД «Об утверждении Устава Государственного бюджетного учреждения города Москвы «Объединение культурных и досуговых центров Северо-Западного административного округа»), **приказываю:**

1. Утвердить и ввести в действие с 22.09.2025 Положение по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в Государственном бюджетном учреждении города Москвы «Объединение культурных и досуговых центров Северо-Западного административного округа» согласно приложению к настоящему приказу.

2. Считать утратившими силу приказ Государственного бюджетного учреждения культуры города Москвы «Объединение культурных центров Северо-Западного административного округа» от 30.08.2022 № 07-98 «Об утверждении Положения о защите и обработке персональных данных работников Государственного бюджетного учреждения культуры города Москвы «Объединение культурных центров Северо-Западного административного округа» и Положение по организации и проведению работ по обеспечению безопасности персональных данных при их обработке ГБУ ЦДМСИ «Крылья» от 29.04.2022.

3. Контроль за исполнением настоящего приказа возложить на заместителя директора по общим вопросам Юнг Т.В.

Директор



Е.Ю.Анашкин

**Положение по организации и проведению работ по обеспечению  
безопасности персональных данных при их обработке  
в Государственном бюджетном учреждении города Москвы  
«Объединение культурных и досуговых центров  
Северо-Западного административного округа»**

## 1. Введение

1.1. Настоящее Положение разработано в соответствии с действующим законодательством Российской Федерации о персональных данных, а именно:

– Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – ФЗ «О персональных данных»), устанавливающим основные принципы и условия обработки персональных данных, права, обязанности и ответственность участников отношений, связанных с обработкой персональных данных;

– Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении Требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– Постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

1.2. Для осуществления мероприятий по обеспечению и контролю безопасности персональных данных, обработки обращений субъектов персональных данных и взаимодействия с уполномоченным органом по защите прав субъектов персональных данных приказом директора Государственного бюджетного учреждения города Москвы «Объединение культурных и досуговых центров Северо-Западного административного округа» (далее – Учреждение) назначаются работники, ответственные за организацию обработки персональных данных и обеспечение безопасности персональных данных.

1.3. Настоящее Положение подлежит пересмотру и при необходимости актуализации в случае изменений в законодательстве Российской Федерации о персональных данных, при изменении организационной структуры Учреждения.

## 2. Общие положения

2.1. Настоящее Положение регламентирует организацию процесса обеспечения безопасности персональных данных в Учреждении

в соответствии с требованиями действующего законодательства в области защиты персональных данных.

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

2.3. Положение обязательно для ознакомления и исполнения работниками Учреждения, ответственными за организацию обработки персональных данных и обеспечение их безопасности.

### **3. Роли персонала**

3.1. Во исполнение положений настоящего документа и соблюдения требований законодательства Российской Федерации о персональных данных в Учреждении введены следующие роли персонала:

- ответственный за организацию обработки персональных данных;
- ответственный за обеспечение безопасности персональных данных.

3.2. Назначение работников ответственными за организацию обработки персональных данных и за обеспечение безопасности персональных данных осуществляется на основании приказа директора Учреждения.

### **4. Обязательные мероприятия по обеспечению безопасности информационных систем персональных данных**

4.1. Общие требования к мероприятиям по обеспечению безопасности информационных систем персональных данных.

4.1.1. Для всех эксплуатируемых информационных систем персональных данных с автоматизированной обработкой персональных данных должны быть определены уровни защищенности персональных данных в соответствии с Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении Требований к защите персональных данных при их обработке в информационных системах персональных данных».

4.1.2. По согласованию с Учредителем (префектурой Северо-Западного административного округа города Москвы) в Учреждении могут использоваться собственные информационные системы персональных данных. Порядок ввода в эксплуатацию и вывода из эксплуатации таких информационных систем приведен в приложении № 4 к настоящему Положению.

4.1.3. В случае создания новых информационных систем персональных данных, расширения состава данных в существующих системах персональных

данных, модернизации систем персональных данных, работы проводятся в следующей последовательности:

4.1.3.1. На этапе создания информационных систем или в ходе их эксплуатации (для ранее введенных в эксплуатацию и/или модернизируемых информационных систем) приказом директора Учреждения создается комиссия по определению уровней защищенности персональных данных в информационных системах персональных данных.

4.1.3.2. Комиссия в установленный приказом срок определяет категории, принадлежность и объем обрабатываемых персональных данных в информационных системах персональных данных, а также определяет типы актуальных угроз безопасности персональных данных, связанных с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении.

4.1.3.3. Комиссия формирует акты определения уровней защищенности персональных данных для каждой информационной системы персональных данных, в которых указываются типы угроз безопасности персональных данных, перечень обрабатываемых категорий персональных данных, их принадлежность и количество записей, содержащих персональные данные.

4.1.4. В Учреждении должны быть разработаны модели угроз безопасности персональных данных для всех информационных систем персональных данных. Модель угроз разрабатывается на основе методических документов, утвержденных в соответствии с ч. 5 ст. 19 ФЗ «О персональных данных».

4.1.5 Выбор и реализация методов и способов защиты информации в информационных системах персональных данных осуществляются на основе модели угроз информационной безопасности и в зависимости от уровня защищенности персональных данных в информационных системах персональных данных.

4.1.6. Выбранные и реализованные методы и способы защиты персональных данных в информационных системах персональных данных должны обеспечивать нейтрализацию выявленных угроз безопасности персональных данных при их обработке в информационных системах персональных данных в составе системы защиты персональных данных.

4.1.7. Для проведения работ по выбору и реализации методов и способов защиты персональных данных (включая техническое проектирование системы защиты персональных данных, внедрение средств защиты персональных данных, сопровождение средств защиты персональных данных и т. д.) могут привлекаться подрядные организации, имеющие лицензию на осуществление деятельности по технической защите конфиденциальной информации.

4.1.8. Общие технические требования по защите персональных данных в информационных системах персональных данных Учреждения приведены в разделе 5.

## 5. Обеспечение технической защиты персональных данных

5.1. Общие требования к обеспечению технической защиты персональных данных в Учреждении.

5.1.1. Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных должно осуществляться на всех стадиях жизненного цикла информационных систем персональных данных и состоять из согласованных мероприятий, направленных на предотвращение (нейтрализацию) и устранение угроз безопасности персональных данных в информационных системах персональных данных, минимизацию возможного ущерба, а также мероприятий по восстановлению данных и нормального функционирования информационных систем персональных данных в случае реализации угроз.

5.1.2. В целях защиты персональных данных от несанкционированного доступа и иных неправомерных действий мероприятия по организации и техническому обеспечению безопасности персональных данных для каждой информационной системы персональных данных должны включать:

5.1.2.1. Определение уровней защищенности персональных данных в информационной системе персональных данных на основании Постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Требования к защите персональных данных при их обработке в информационных системах персональных данных».

5.1.2.2. Выявление и закрытие технических каналов утечки персональных данных на основе анализа и актуализации модели угроз безопасности персональных данных.

5.1.2.3. Выбор и реализацию организационных и технических методов и способов защиты информации в информационной системе в зависимости от уровня защищенности персональных данных в информационной системе персональных данных с учетом особенностей инфраструктуры и с учетом актуальных угроз безопасности персональных данных в информационной системе персональных данных.

5.1.2.4. Установку, настройку и применение соответствующих программных, аппаратных и программно-аппаратных средств защиты информации.

5.1.2.5. Разработку обязанностей работников по обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных для персонала, задействованного в эксплуатации данной информационной системы персональных данных.

5.1.3. Предотвращение утечки персональных данных по техническим каналам за счет побочных электромагнитных излучений и наводок, а также за счет электроакустических преобразований реализуется в Учреждении организационными мерами и не требует специальных технических решений.

5.1.4. Защита персональных данных при их обработке в информационной системе персональных данных от несанкционированного

доступа и иных неправомерных действий должна осуществляться в Учреждении следующими методами и способами:

5.1.4.1. Реализация разрешительной системы допуска пользователей (обслуживающего персонала) к информационным ресурсам (включая персональные данные) информационной системы персональных данных и связанным с ее использованием работам.

5.1.4.2. Ограничение доступа пользователей в помещения Учреждения, где размещены технические средства, позволяющие осуществлять обработку персональных данных, а также хранятся носители информации, содержащие персональные данные.

5.1.4.3. Разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам (включая персональные данные), программным средствам обработки (передачи) и защиты персональных данных.

5.1.4.4. Регистрация действий пользователей и обслуживающего персонала информационной системы персональных данных, мониторинг попыток несанкционированного доступа.

5.1.4.5. Учет и хранение съемных носителей информации с персональными данными и их обращение, исключая хищение, подмену и уничтожение.

5.1.4.6. Использование защищенных каналов связи, используемых для передачи персональных данных.

5.1.4.7. Размещение технических средств, позволяющих осуществлять обработку персональных данных, в пределах контролируемой территории.

5.1.4.8. Предотвращение внедрения в информационную систему персональных данных вредоносных программ (программ-вирусов) и программных закладок.

5.1.4.9. Регистрация событий и мониторинг процессов обработки информации.

5.1.4.10. Контроль целостности программных средств.

5.1.4.11. Регистрация запуска (остановки) программ обработки персональных данных.

5.1.4.12. Регистрация вывода персональных данных на печать.

5.1.5. При организации взаимодействия информационной системы персональных данных с информационно-телекоммуникационными сетями международного информационного обмена (сетями связи общего пользования) наряду с указанными методами и способами должны применяться следующие дополнительные методы и способы защиты персональных данных от несанкционированного доступа:

5.1.5.1. Межсетевое экранирование с целью управления доступом, фильтрации сетевых пакетов и трансляции сетевых адресов для скрывания структуры информационной системы персональных данных.

5.1.5.2. Защита персональных данных при их передаче по каналам связи.

5.1.5.3. Использование смарт-карт, электронных замков и других носителей информации для надежной идентификации и аутентификации пользователей.

5.1.5.4. Использование средств антивирусной защиты.

5.1.6. К событиям безопасности в информационной системе персональных данных относятся следующие события:

5.1.6.1. Доступ (входа и выхода в систему и доступа к объектам, в том числе неудачные попытки доступа).

5.1.6.2. Создание и удаление пользователей.

5.1.6.3. Изменение прав доступа и привилегий.

5.1.6.4. Подключение и отключение внешних устройств.

5.1.6.5. Изменение настроек средств защиты.

5.1.6.6. События, генерируемые средствами защиты.

5.1.7. В Учреждении также могут разрабатываться и применяться другие методы защиты информации от несанкционированного доступа, обеспечивающие нейтрализацию угроз безопасности персональных данных.

5.1.8. Конкретные методы и средства защиты персональных данных в информационной системе персональных данных должны определяться на основании нормативно-методических документов ФСТЭК России и ФСБ России, исходя из уровней защищенности персональных данных в информационной системе персональных данных и актуальных угроз безопасности персональных данных.

5.1.9. Все технические средства защиты информации должны быть снабжены инструкциями по эксплуатации.

5.2. Контроль выполнения требований по защите персональных данных.

5.2.1. В соответствии с документом «Требования к защите персональных данных при их обработке в информационных системах персональных данных», утвержденным Постановлением Правительства Российской Федерации от 01.11.2012 № 1119, должен проводиться периодический контроль выполнения требований по обеспечению безопасности персональных данных (не реже одного раза в три года).

5.2.2. Контроль функций системы защиты производится в рамках мероприятий, описанных в пункте 7.2 настоящего Положения.

5.2.3. Ответственность за контроль функций системы защиты персональных данных возлагается на ответственного за обеспечение безопасности персональных данных.

5.3. Учет съемных электронных носителей персональных данных.

5.3.1. В Учреждении должен вестись учет защищаемых съемных носителей персональных данных, к которым относятся:

– носители информации серверов;

– носители информации автоматизированного рабочего места;

– внешние запоминающие устройства (флеш-накопители, карты памяти и т. п.), содержащие персональные данные.

5.3.2. Ответственность за учет защищаемых электронных носителей персональных данных возлагается на ответственного за обеспечение безопасности персональных данных.

## **6. Обязанности персонала**

6.1. В обязанности ответственного за организацию обработки персональных данных входит:

6.1.1. Осуществление внутреннего контроля за соблюдением Учреждением и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных.

6.1.2. Доведение до сведения работников Учреждения положений законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных.

6.1.3. Прием и обработка обращений субъектов персональных данных и их законных представителей (ведение журнала учета обращений субъектов персональных данных, анализ правомерности запросов, составление и отправка ответов).

6.1.4. Прием и обработка запросов уполномоченного органа по защите прав субъектов персональных данных (анализ правомерности запросов, составление и отправка ответов).

6.1.5. Уведомление уполномоченного органа по защите прав субъектов персональных данных об обработке персональных данных, об изменениях в реквизитах оператора персональных данных.

6.1.6. Уведомление уполномоченного органа по защите прав субъектов персональных данных по запросу этого органа с предоставлением необходимой информации в течение тридцати дней с даты получения такого запроса.

6.2. Ответственный за организацию обработки персональных данных обладает следующими полномочиями:

6.2.1. Запрашивать необходимую информацию у руководства и работников Учреждения, относящуюся к обработке персональных данных и необходимую для выполнения его обязанностей.

6.2.2. Контролировать выполнение обязанностей ответственным за обеспечение безопасности персональных данных, а также выполнение требований законодательства и внутренних нормативных документов Учреждения, регламентирующих обработку и обеспечение безопасности персональных данных.

6.2.3. Назначать ответственного за уничтожение персональных данных и контролировать выполнение процедуры уничтожения персональных данных.

6.2.4. Согласовывать заявки временного или разового допуска работника к работе с персональными данными в связи со служебной необходимостью.

6.3. Обязанности ответственного за обеспечение безопасности персональных данных:

6.3.1. Предоставление и прекращение доступа пользователей к персональным данным в информационных системах персональных данных работникам, допущенным к работе с персональными данными;

6.3.2. Управление учетными записями пользователей комплекса информационных систем персональных данных.

6.3.3. Проведение контрольных мероприятий.

6.3.4. Предоставление сведений о персональных данных ответственному за организацию обработки персональных данных в рамках проведения учета защищаемых носителей и проведения инвентаризации.

6.3.5. Установка, конфигурирование и администрирование аппаратных и программных средств защиты информации комплекса информационных систем персональных данных.

6.3.6. Поддержание штатной работы комплекса информационных систем персональных данных.

6.3.7. Учет защищаемых носителей персональных данных.

6.3.8. Учет технических средств защиты информации.

6.3.9. Анализ защищенности информационных систем персональных данных.

6.3.10. Организация процесса обучения работников по направлению обеспечения безопасности персональных данных.

6.3.11. Участие в проведении внутреннего контроля и служебных расследований фактов нарушения установленного порядка обработки и обеспечения безопасности персональных данных.

6.4. Ответственный за обеспечение безопасности персональных данных обладает следующими полномочиями:

6.4.1. Проводит плановые и внеплановые контрольные мероприятия в целях контроля, изучения и оценки фактического состояния защищенности персональных данных;

6.4.2. Запрашивает необходимую информацию у работников Учреждения по фактам нарушения установленного порядка обработки и обеспечения безопасности персональных данных.

## **7. Организация внутреннего контроля обработки и обеспечения безопасности персональных данных**

7.1. Цели организации внутреннего контроля.

7.1.1. Организация внутреннего контроля процесса обработки персональных данных в Учреждении осуществляется в целях изучения и оценки фактического состояния защищенности персональных данных, своевременного реагирования на нарушения установленного порядка

их обработки, а также в целях совершенствования этого порядка и обеспечения его соблюдения.

7.1.2. Мероприятия по осуществлению внутреннего контроля обработки и обеспечения безопасности персональных данных направлены на решение следующих задач:

7.1.2.1. Обеспечение соблюдения работниками Учреждения требований настоящего Положения и нормативных правовых актов, регулирующих защиту персональных данных.

7.1.2.2. Оценка компетентности персонала, задействованного в обработке персональных данных.

7.1.2.3. Обеспечение работоспособности и эффективности технических средств информационных систем персональных данных и средств защиты персональных данных, их соответствия требованиям уполномоченных органов исполнительной власти по вопросам безопасности персональных данных.

7.1.2.4. Выявление нарушений установленного порядка обработки персональных данных и своевременное предотвращение негативных последствий таких нарушений.

7.1.2.5. Принятие корректирующих мер, направленных на устранение выявленных нарушений в порядке обработки персональных данных, а также в работе технических средств информационных систем персональных данных.

7.1.2.6. Разработка рекомендаций по совершенствованию порядка обработки и обеспечения безопасности персональных данных по результатам контрольных мероприятий.

7.1.2.7. Осуществление контроля исполнения рекомендаций и указаний по устранению нарушений.

7.2. Проведение контрольных мероприятий.

7.2.1. Контрольные мероприятия (проверки) проводятся на плановой основе, а также при необходимости внепланово.

7.2.2. Решение о необходимости проведения внеплановых контрольных мероприятий принимает ответственный за обеспечение безопасности персональных данных. Данное решение должно быть обосновано возросшими рисками информационной безопасности для обрабатываемых персональных данных и при существенных изменениях в среде обработки персональных данных.

7.2.3. Контрольные мероприятия (проверки) организуются ответственным за обеспечение безопасности персональных данных.

7.2.4. Плановые проверки проводятся не реже одного раза в полугодие и включают в себя:

7.2.4.1. Проверку деятельности работников Учреждения, допущенных к работе с персональными данными в информационных системах персональных данных, на соответствие осуществляемого порядка обработки и обеспечения безопасности персональных данных порядку, установленному локальными документами Учреждения.

7.2.4.2. Проверку работоспособности и эффективности технических средств информационных систем персональных данных и средств защиты персональных данных.

7.2.4.3. Проверку ведения эталонных копий средств защиты.

7.2.4.4. Проверку соответствия предоставленных прав доступа пользователей к персональным данным утвержденной матрице доступа.

7.2.4.5. Проверку минимальной длины и сложности паролей.

7.2.4.6. Проверку периодичности смены паролей.

7.2.4.7. Проверку отсутствия на автоматизированных рабочих местах пользователей средств разработки.

7.2.4.8. Проверку отсутствия на автоматизированных рабочих местах пользователей штатного программного обеспечения.

7.2.4.9. Мониторинг журналов протоколирования событий аутентификации.

7.2.5. По фактам выявленных нарушений проводится служебное расследование в соответствии с порядком, предусмотренным пунктом 7.3 настоящего Положения.

7.2.6. При необходимости предлагаются меры по минимизации последствий выявленных угроз информационной безопасности.

7.2.7. В случае передачи части функций в области информационных технологий сторонним организациям, указанные контрольные мероприятия осуществляют эти сторонние организации. Требования по осуществлению контрольных мероприятий указываются в договорах с этими сторонними организациями.

7.3. Порядок проведения служебных расследований.

7.3.1. Проведение служебных расследований может быть инициировано в одном из следующих случаев:

7.3.1.1. Обращение субъекта персональных данных по поводу неправомерных действий в отношении его персональных данных.

7.3.1.2. Выявление нарушений работниками Учреждения в рамках выполнения своих должностных обязанностей, связанных с обработкой или защитой персональных данных.

7.3.1.3. Выявление нарушений, приводящих к снижению уровня защищенности персональных данных, в ходе проведения проверок состояния защищенности персональных данных.

7.3.2. В ходе проведения служебного расследования ответственный за обеспечение безопасности персональных данных устанавливает обстоятельства допущенного нарушения.

7.3.3. В ходе проведения служебного расследования выясняется:

7.3.3.1. Дата и время совершения нарушения.

7.3.3.2. Обстоятельства, при которых были совершены действия, приведшие к возникновению нарушения.

7.3.3.3. Последствия, возникшие вследствие совершения нарушения.

7.3.4. Работники Учреждения должны предоставить объяснительные записки по фактам выявленных в ходе служебного расследования нарушений.

7.3.5. Ответственный за обеспечение безопасности персональных данных оценивает последствия, возникшие вследствие совершения нарушения.

7.3.6. По результатам служебного расследования составляется акт, который содержит:

7.3.6.1. Краткую справку по нарушению, в отношении которого проводилось разбирательство.

7.3.6.2. Данные о работнике Учреждения, допустившем нарушение.

7.3.6.3. Информацию о привлечении работника Учреждения к дисциплинарной ответственности.

Приложение № 1  
к Положению по организации  
и проведению работ  
по обеспечению безопасности  
персональных данных  
при их обработке в Государственном  
бюджетном учреждении города  
Москвы «Объединение культурных  
и досуговых центров  
Северо-Западного  
административного округа»

## Форма согласия потребителя услуг на обработку и распространение персональных данных

### СОГЛАСИЕ НА ОБРАБОТКУ И РАСПРОСТРАНЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Я, Заказчик (ФИО) \_\_\_\_\_,  
проживающий по адресу \_\_\_\_\_,  
паспорт серия \_\_\_\_\_ № \_\_\_\_\_ выдан (кем) \_\_\_\_\_,  
\_\_\_\_\_ выдан (когда) \_\_\_\_\_, тел.: \_\_\_\_\_.

Настоящим даю свое согласие на обработку в ГБУ г. Москвы «ОКЦ СЗАО» (далее – Учреждение) персональных данных Потребителя услуг (для целей настоящего Соглашения понятия «Заказчик» и «Потребитель услуг» являются тождественными и используются как равнозначные, если Заказчик лично посещает занятия в клубном формировании/спортивной секции) \_\_\_\_\_,

относящихся исключительно к перечисленным ниже категориям персональных данных Заказчика/Потребителя услуг:

- данные документа, удостоверяющего личность/данные свидетельства о рождении: ФИО, пол, дата рождения, тип, серия, номер документа, удостоверяющего личность, кем и когда выдан, гражданство, СНИЛС;
- медицинские сведения: данные медицинской карты (справки); сведения о состоянии здоровья; отнесение к категории лиц с ОВЗ, детей-инвалидов; сведения о прохождении медосмотров; сведения о наличии заключения ЦПМПК;
- адрес проживания/регистрации, номер телефона и адрес электронной почты;
- фото- и видеоизображение.

Я даю согласие на использование персональных данных исключительно в следующих целях:

- обеспечения защиты конституционных прав и свобод Заказчика/Потребителя услуг;
- обеспечения соблюдения нормативных правовых актов Российской Федерации и города Москвы;
- обеспечения безопасности посещающего в период нахождения на территории Учреждения;
- обеспечения организации деятельности Учреждения, культурно-досуговых, физкультурных, спортивно-массовых и иных мероприятий;
- ведения статистики;
- размещения фотоизображения на официальном сайте Учреждения и социальных сетях в рамках организации деятельности Учреждения, культурно-досуговых, физкультурных, спортивно-массовых и иных мероприятий;
- видеосъемки и размещения видеоматериалов на официальном сайте Учреждения, социальных сетях в рамках деятельности Учреждения, культурно-досуговых, физкультурных, спортивно-массовых и иных мероприятий;
- контроля за посещениями занятий.

Настоящее согласие предоставляется на осуществление сотрудниками Учреждения следующих действий в отношении персональных данных Заказчика/Потребителя услуг: сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование (только в указанных выше целях), обезличивание, блокирование (не включает возможность ограничения доступа Заказчика к персональным данным Потребителя услуг), а также осуществление любых иных действий, предусмотренных действующим законодательством Российской Федерации.

Я не даю согласия на какое-либо распространение персональных данных Потребителя услуг, в том числе на передачу персональных данных Заказчика/Потребителя услуг каким-либо третьим лицам, включая физических и юридических лиц, государственные органы и органы местного самоуправления, за исключением передачи персональных данных следующим организациям:

- Департаменту информационных технологий города Москвы, в том числе подведомственным ему организациям;
- Департаменту культуры города Москвы;

- Государственному казенному учреждению города Москвы «Информационный город»;
- Государственному бюджетному учреждению культуры города Москвы «Московская дирекция по развитию культурных центров», с целью предоставления доступа к информационным ресурсам государственной информационной системы «Портал государственных и муниципальных услуг (функций) города Москвы»;
- АНО «Московский Спорт»;
- Департаменту спорта города Москвы;
- ГБУ «МОСГОРСПОРТ» Москомспорта;
- Префектуре Северо-Западного административного округа города Москвы.

Обработка персональных данных должна осуществляться с соблюдением требований, установленных законодательством Российской Федерации и только для целей, указанных выше. Учреждение обязано осуществлять защиту персональных данных Заказчика/Потребителя услуг, принимать необходимые организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, модифицирования, блокирования, копирования, распространения, а также от иных неправомерных действий в отношении данной информации.

Обработка персональных данных Заказчика/Потребителя услуг для любых иных целей и любым иным способом, включая распространение и передачу их иным лицам или иное их разглашение может осуществляться только с моего особого письменного согласия в каждом отдельном случае.

Защита внесенной информации осуществляется с соблюдением требований, установленных законодательством Российской Федерации. Хранение и обработка информации, а также обмен информацией осуществляются после принятия необходимых мер по защите указанной информации. В случае нарушения требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» Учреждение несет ответственность, предусмотренную Кодексом РФ об административных правонарушениях, Трудовым кодексом РФ, Уголовным кодексом РФ.

Данное согласие действует до достижения целей обработки персональных данных в Учреждении или до истечения срока хранения информации данного согласия. Данное согласие может быть отозвано в любой момент по моему письменному заявлению.

Мне разъяснено, что отзыв настоящего согласия может затруднить или сделать невозможным возобновление обработки персональных данных и их подтверждение.

Я подтверждаю, что, давая настоящее согласие, я действую по своей воле и в интересах Потребителя услуг.

Дата: \_\_\_\_ . \_\_\_\_ 202\_\_ г.

Подпись Заказчика: \_\_\_\_\_

Приложение № 2  
к Положению по организации  
и проведению работ  
по обеспечению безопасности  
персональных данных  
при их обработке в Государственном  
бюджетном учреждении города  
Москвы «Объединение культурных  
и досуговых центров  
Северо-Западного  
административного округа»

## Форма согласия работника на обработку его персональных данных

### СОГЛАСИЕ НА ОБРАБОТКУ И РАСПРОСТРАНЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Я, \_\_\_\_\_,  
(фамилия, имя, отчество полностью)

зарегистрированный по адресу \_\_\_\_\_

\_\_\_\_\_, паспорт серия \_\_\_\_\_ № \_\_\_\_\_,

выдан (кем, когда) \_\_\_\_\_

даю свое согласие ГБУ г. Москвы «ОКЦ СЗАО» на обработку своих персональных данных в целях:

- обеспечения защиты моих конституционных прав и свобод;
- обеспечения соблюдения законов и иных нормативных правовых актов;
- заключения и регулирования трудовых отношений и иных непосредственно связанных с ними отношений;
- отражения информации в кадровых документах;
- начисления заработной платы;
- предоставления льгот, предусмотренных трудовым и налоговым законодательствами;
- исчисления и уплаты, предусмотренных законодательством РФ налогов, сборов и взносов на обязательное социальное и пенсионное страхование;
- представления работодателем установленной законодательством отчетности в отношении физических лиц, в том числе в Социальный фонд России и ФНС России;
- перечисления заработной платы;
- предоставления налоговых вычетов;
- обеспечения моей безопасности;
- оперативного доведения до меня информации со стороны ГБУ г. Москвы «ОКЦ СЗАО»;
- контроля количества и оценки качества выполняемой мной работы;
- размещения фото- и видеоизображений на официальном сайте и социальных сетях ГБУ г. Москвы «ОКЦ СЗАО» для освещения информации.

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

- фамилия, имя, отчество;
- пол, возраст;
- дата и место рождения, гражданство;
- паспортные данные (серия, номер, кем и когда выдан);
- фото-, видеоизображения;
- сведения о социальных льготах, о состоянии здоровья, о результатах медицинских осмотров и о профилактических прививках;
- сведения о временной нетрудоспособности, о характере полученных травм на работе;
- наличие (отсутствие) судимости и (или) факта уголовного преследования;
- сведения об условиях труда на рабочем месте;
- адрес регистрации по месту жительства и адрес фактического проживания;
- номер телефона (домашний, мобильный) и адрес электронной почты;
- сведения об образовании (квалификация, профессиональная подготовка, повышение квалификации);
- результаты прохождения аттестации;
- семейное положение, состав семьи;

- отношение к воинской обязанности;
- сведения о трудовом стаже, наличие наград, поощрений и почетных званий, предыдущих местах работы, доходах с предыдущих мест работы;
- должность;
- размер заработной платы;
- сведения об открытых банковских счетах, на которые перечисляется заработная плата в ГБУ г. Москвы «ОКЦ СЗАО»:

- сведения о налоговых отчислениях и сборах;
- номер СНИЛС;
- ИНН;
- информация о приеме, переводе, увольнении и иных событиях, относящихся к моей трудовой деятельности в ГБУ г. Москвы «ОКЦ СЗАО»;
- сведения о доходах в ГБУ г. Москвы «ОКЦ СЗАО»;
- сведения о деловых и иных личных качествах, носящих оценочный характер.

Я не даю согласия на какое-либо распространение моих персональных данных и их передачу третьим лицам, включая физических и юридических лиц государственных органов и органов местного самоуправления, за исключением передачи персональных данных следующим организациям:

- Департамент информационных технологий города Москвы, в том числе подведомственные ему организации;
- Федеральная служба по труду и занятости;
- Социальный фонд России;
- Федеральная налоговая служба России;
- Префектура Северо-Западного административного округа города Москвы.

Обработка персональных данных должна осуществляться с соблюдением требований, установленных законодательством Российской Федерации и только для целей, указанных выше. ГБУ г. Москвы «ОКЦ СЗАО» обязано осуществлять защиту моих персональных данных, принимать необходимые организационные и технические меры для защиты моих персональных данных от неправомерного или случайного доступа к ним, уничтожения, модифицирования, блокирования, копирования, распространения, обезличивание, а также от иных неправомерных действий в отношении данной информации.

Обработка моих персональных данных для любых иных целей и любым иным способом, включая распространение и передачу их иным лицам, или иное их разглашение, может осуществляться только с моего письменного согласия в каждом отдельном случае.

Защита внесенной информации должна осуществляться с соблюдением требований, установленных законодательством Российской Федерации. Хранение и обработка информации, а также обмен информацией должны осуществляться после принятия необходимых мер по защите указанной информации. В случае нарушения требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» ГБУ г. Москвы «ОКЦ СЗАО» должно нести ответственность, предусмотренную Кодексом РФ об административных правонарушениях, Трудовым кодексом РФ, Уголовным кодексом РФ.

Данное согласие действует до достижения целей обработки персональных данных в ГБУ г. Москвы «ОКЦ СЗАО» или в течение срока хранения информации. Данное согласие может быть отозвано в любой момент по моему письменному заявлению в его части или полном объеме.

Я подтверждаю, что, давая настоящее согласие, я действую по своей воле и в своих интересах.

Дата: \_\_\_\_\_ г.

Подпись: \_\_\_\_\_ ( \_\_\_\_\_ )

Ф.И.О.

Приложение № 3  
к Положению по организации  
и проведению работ  
по обеспечению безопасности  
персональных данных  
при их обработке в Государственном  
бюджетном учреждении города  
Москвы «Объединение культурных  
и досуговых центров  
Северо-Западного  
административного округа»

### Форма акта об уничтожении персональных данных

«УТВЕРЖДАЮ»

\_\_\_\_\_ 202\_ г.

Акт № \_\_\_\_\_  
об уничтожении персональных данных

№ п/п	Дата	Место и форма хранения персональных данных	Тип носителя персональных данных и его регистрационный номер/уничтожаемые персональные данные

Всего уничтожено носителей (прописью): \_\_\_\_\_

Уничтожение произведено путем

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_.

Ответственный за уничтожение (Ф.И.О., должность): \_\_\_\_\_.

Дата: \_\_\_\_\_.

Подпись: \_\_\_\_\_.

Приложение № 4  
к Положению по организации  
и проведению работ  
по обеспечению безопасности  
персональных данных  
при их обработке в Государственном  
бюджетном учреждении города  
Москвы «Объединение культурных  
и досуговых центров  
Северо-Западного  
административного округа»

## **Порядок ввода в эксплуатацию и вывода из эксплуатации информационных систем персональных данных**

### **1. Требования к разработке и вводу в эксплуатацию информационных систем персональных данных**

1.1. Разработка информационной системы персональных данных должна включать следующие стадии:

- предпроектная стадия, которая включает предварительный анализ целей и условий функционирования информационной системы персональных данных, а также обрабатываемых в ней персональных данных, на основании которого определяется предварительный класс информационной системы персональных данных, степень участия должностных лиц, актуализация угрозы безопасности;
- стадия проектирования системы защиты персональных данных для информационной системы персональных данных;
- стадия ввода в действие информационной системы персональных данных.

1.2. По результатам проведенного анализа и с учетом действующих требований законодательства Российской Федерации о персональных данных и регуляторов должны быть разработаны:

- модель угроз безопасности персональных данных при их обработке в информационной системе персональных данных;
- акт об установлении уровня защищенности персональных данных в информационной системе персональных данных;
- требования к защите персональных данных при их обработке в информационной системе персональных данных;
- техническое задание на создание системы защиты персональных данных для информационной системы персональных данных.

1.3. При определении отсутствия недекларированных возможностей в системном и/или прикладном программном обеспечении выполняются

следующие мероприятия для подтверждения типа угроз безопасности персональных данных в информационной системе персональных данных:

- проверка системного и/или прикладного программного обеспечения, включая программный код, на отсутствие недеklarированных возможностей с использованием автоматизированных средств и/или без их использования;
- тестирование информационной системы на несанкционированные проникновения;
- использование в информационной системе системного и/или прикладного программного обеспечения, разработанного с использованием методов защищенного программирования.

1.4. Проектирование системы защиты персональных данных для вводимой в эксплуатацию информационной системы персональных данных должно производиться с учетом уже построенной в Учреждении системы защиты персональных данных, включающей комплекс организационных и технических мер.

1.5. На стадии ввода в эксплуатацию информационной системы персональных данных должны быть проведены следующие мероприятия:

- установка пакета прикладных программ информационной системы персональных данных совместно со средствами защиты информации (встроенными и наложенными);
- опытная эксплуатация средств защиты информации в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в составе информационной системы персональных данных;
- испытания по приемке-сдаче средств защиты информации по результатам опытной эксплуатации.

1.6. В случае внедрения дополнительных средств защиты по результатам приемо-сдаточных испытаний должны быть составлены акты внедрения средств защиты информации, подготавливаемые и подписываемые ответственным за обеспечение безопасности персональных данных.

1.7. Перед вводом новой информационной системы персональных данных в опытную эксплуатацию должен быть составлен акт о вводе в опытную эксплуатацию информационной системы персональных данных, подписываемый ответственным за обеспечение безопасности персональных данных, а также акт определения уровней защищенности персональных данных в информационной системе персональных данных, подготовленный и подписанный комиссией по определению уровней защищенности персональных данных в информационной системе персональных данных.

1.8. В случае успешного функционирования информационной системы персональных данных на стадии опытной эксплуатации и принятия решения о переводе ее в промышленную эксплуатацию составляется акт о вводе в промышленную эксплуатацию новой информационной системы персональных данных.

## **2. Требования к выводу информационной системы персональных данных из эксплуатации**

2.1. В случае принятия решения о выводе информационной системы персональных данных из эксплуатации, ответственным за обеспечение безопасности персональных данных и директором Учреждения должен быть подписан акт о выводе информационной системы персональных данных из эксплуатации.

2.2. При выводе информационной системы персональных данных из эксплуатации с целью обеспечения справочной поддержки Учреждения, доступ к ней должен быть ограничен определенным составом лиц с правами только на чтение.

2.3. После подписания акта о выводе информационной системы персональных данных из эксплуатации, информационная система персональных данных переводится в архивный фонд Учреждения (в соответствии с ч. 2 ст. 13 ФЗ «Об архивном деле»), при этом должны быть выполнены следующие требования:

- доступ к архивной информационной системе персональных данных и хранимым в ней документам должен обеспечиваться на основании соответствующей заявки на имя руководства Учреждения, по согласованию с ответственным за организацию обработки персональных данных и владельцем информационной системы персональных данных;

- персональные данные, хранящиеся в архиве, могут быть использованы и переданы третьим лицам только в целях исполнения законодательства Российской Федерации;

- должны быть обеспечены финансовые, материально-технические и иные условия, необходимые для комплектования, хранения, учета и использования информационной системы персональных данных, включая специальное помещение, отвечающее нормативным условиям труда работников архива;

- доступ в помещения, где предполагается хранение выводимой из эксплуатации информационной системы персональных данных, должен быть ограничен;

- должен быть регламентирован перечень лиц, допущенных к работе с информационной системой персональных данных, переданной в архив;

- все внешние запоминающие устройства (ленты с резервными копиями, дискеты, CD-диски, флеш-накопители и т. п.) должны храниться в сейфах;

- должно быть разработано описание информационной системы персональных данных, переведенной в архивный фонд Учреждения. Описание информационной системы персональных данных разрабатывается ответственным за обеспечение безопасности либо сторонней компанией, имеющей лицензию ФСТЭК России на осуществление технической защиты информации.

Приложение № 1  
к Положению по организации  
и проведению работ  
по обеспечению безопасности  
персональных данных  
при их обработке в Государственном  
бюджетном учреждении города  
Москвы «Объединение культурных  
и досуговых центров  
Северо-Западного  
административного округа»

**Форма согласия потребителя услуг  
на обработку и распространение персональных данных**

**СОГЛАСИЕ НА ОБРАБОТКУ И РАСПРОСТРАНЕНИЕ  
ПЕРСОНАЛЬНЫХ ДАННЫХ**

Я, Заказчик (ФИО) \_\_\_\_\_,  
проживающий по адресу \_\_\_\_\_,  
паспорт серия \_\_\_\_\_ № \_\_\_\_\_ выдан (кем) \_\_\_\_\_,  
\_\_\_\_\_ выдан (когда) \_\_\_\_\_, тел.: \_\_\_\_\_.

Настоящим даю свое согласие на обработку в ГБУ г. Москвы «ОКЦ СЗАО» (далее – Учреждение) персональных данных Потребителя услуг (для целей настоящего Соглашения понятия «Заказчик» и «Потребитель услуг» являются **тождественными и используются как равнозначные**, если Заказчик **лично** посещает занятия в клубном формировании/спортивной секции) \_\_\_\_\_,

относящихся исключительно к перечисленным ниже категориям персональных данных Заказчика/Потребителя услуг:

- данные документа, удостоверяющего личность/данные свидетельства о рождении: ФИО, пол, дата рождения, тип, серия, номер документа, удостоверяющего личность, кем и когда выдан, гражданство, СНИЛС;
- медицинские сведения: данные медицинской карты (справки); сведения о состоянии здоровья; отнесение к категории лиц с ОВЗ, детей-инвалидов; сведения о прохождении медосмотров; сведения о наличии заключения ЦПМПК;
- адрес проживания/регистрации, номер телефона и адрес электронной почты;
- фото- и видеоизображение.

Я даю согласие на использование персональных данных исключительно в следующих целях:

- обеспечения защиты конституционных прав и свобод Заказчика/Потребителя услуг;
- обеспечения соблюдения нормативных правовых актов Российской Федерации и города Москвы;
- обеспечения безопасности посещающего в период нахождения на территории Учреждения;
- обеспечения организации деятельности Учреждения, культурно-досуговых, физкультурных, спортивно-массовых и иных мероприятий;
- ведения статистики;
- размещения фотоизображения на официальном сайте Учреждения и социальных сетях в рамках организации деятельности Учреждения, культурно-досуговых, физкультурных, спортивно-массовых и иных мероприятий;
- видеосъемки и размещения видеоматериалов на официальном сайте Учреждения, социальных сетях в рамках деятельности Учреждения, культурно-досуговых, физкультурных, спортивно-массовых и иных мероприятий;
- контроля за посещения занятия.

Настоящее согласие предоставляется на осуществление сотрудниками Учреждения следующих действий в отношении персональных данных Заказчика/Потребителя услуг: сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование (только в указанных выше целях), обезличивание, блокирование (не включает возможность ограничения доступа Заказчика к персональным данным Потребителя услуг), а также осуществление любых иных действий, предусмотренных действующим законодательством Российской Федерации.

Я не даю согласия на какое-либо распространение персональных данных Потребителя услуг, в том числе на передачу персональных данных Заказчика/Потребителя услуг каким-либо третьим лицам, включая физических и юридических лиц, государственные органы и органы местного самоуправления, за исключением передачи персональных данных следующим организациям:

- Департаменту информационных технологий города Москвы, в том числе подведомственным ему организациям;
- Департаменту культуры города Москвы;

- Государственному казенному учреждению города Москвы «Информационный город»;
- Государственному бюджетному учреждению культуры города Москвы «Московская дирекция по развитию культурных центров», с целью предоставления доступа к информационным ресурсам государственной информационной системы «Портал государственных и муниципальных услуг (функций) города Москвы»;
- АНО «Московский Спорт»;
- Департаменту спорта города Москвы;
- ГБУ «МОСГОРСПОРТ» Москомспорта;
- Префектуре Северо-Западного административного округа города Москвы.

Обработка персональных данных должна осуществляться с соблюдением требований, установленных законодательством Российской Федерации и только для целей, указанных выше. Учреждение обязано осуществлять защиту персональных данных Заказчика/Потребителя услуг, принимать необходимые организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, модифицирования, блокирования, копирования, распространения, а также от иных неправомерных действий в отношении данной информации.

Обработка персональных данных Заказчика/Потребителя услуг для любых иных целей и любым иным способом, включая распространение и передачу их иным лицам или иное их разглашение может осуществляться только с моего особого письменного согласия в каждом отдельном случае.

Защита внесенной информации осуществляется с соблюдением требований, установленных законодательством Российской Федерации. Хранение и обработка информации, а также обмен информацией осуществляются после принятия необходимых мер по защите указанной информации. В случае нарушения требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» Учреждение несет ответственность, предусмотренную Кодексом РФ об административных правонарушениях, Трудовым кодексом РФ, Уголовным кодексом РФ.

Данное согласие действует до достижения целей обработки персональных данных в Учреждении или до истечения срока хранения информации данного согласия. Данное согласие может быть отозвано в любой момент по моему письменному заявлению.

Мне разъяснено, что отзыв настоящего согласия может затруднить или сделать невозможным возобновление обработки персональных данных и их подтверждение.

Я подтверждаю, что, давая настоящее согласие, я действую по своей воле и в интересах Потребителя услуг.

Дата: \_\_\_\_ . \_\_\_\_ 202\_\_ г.

Подпись Заказчика: \_\_\_\_\_

Приложение № 2  
к Положению по организации  
и проведению работ  
по обеспечению безопасности  
персональных данных  
при их обработке в Государственном  
бюджетном учреждении города  
Москвы «Объединение культурных  
и досуговых центров  
Северо-Западного  
административного округа»

## Форма согласия работника на обработку его персональных данных

### СОГЛАСИЕ НА ОБРАБОТКУ И РАСПРОСТРАНЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Я, \_\_\_\_\_,  
*(фамилия, имя, отчество полностью)*

зарегистрированный по адресу \_\_\_\_\_

\_\_\_\_\_, паспорт серия \_\_\_\_\_ № \_\_\_\_\_

выдан *(кем, когда)* \_\_\_\_\_

даю свое согласие ГБУ г. Москвы «ОКЦ СЗАО» на обработку своих персональных данных в целях:

- обеспечения защиты моих конституционных прав и свобод;
- обеспечения соблюдения законов и иных нормативных правовых актов;
- заключения и регулирования трудовых отношений и иных непосредственно связанных с ними отношений;
- отражения информации в кадровых документах;
- начисления заработной платы;
- предоставления льгот, предусмотренных трудовым и налоговым законодательствами;
- исчисления и уплаты, предусмотренных законодательством РФ налогов, сборов и взносов на обязательное социальное и пенсионное страхование;
- представления работодателем установленной законодательством отчетности в отношении физических лиц, в том числе в Социальный фонд России и ФНС России;
- перечисления заработной платы;
- предоставления налоговых вычетов;
- обеспечения моей безопасности;
- оперативного доведения до меня информации со стороны ГБУ г. Москвы «ОКЦ СЗАО»;
- контроля количества и оценки качества выполняемой мной работы;
- размещения фото- и видеоизображений на официальном сайте и социальных сетях ГБУ г. Москвы «ОКЦ СЗАО» для освещения информации.

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

- фамилия, имя, отчество;
- пол, возраст;
- дата и место рождения, гражданство;
- паспортные данные (серия, номер, кем и когда выдан);
- фото-, видеоизображения;
- сведения о социальных льготах, о состоянии здоровья, о результатах медицинских осмотров и о профилактических прививках;
- сведения о временной нетрудоспособности, о характере полученных травм на работе;
- наличие (отсутствие) судимости и (или) факта уголовного преследования;
- сведения об условиях труда на рабочем месте;
- адрес регистрации по месту жительства и адрес фактического проживания;
- номер телефона (домашний, мобильный) и адрес электронной почты;
- сведения об образовании (квалификация, профессиональная подготовка, повышение квалификации);
- результаты прохождения аттестации;
- семейное положение, состав семьи;

- отношение к воинской обязанности;
- сведения о трудовом стаже, наличие наград, поощрений и почетных званий, предыдущих местах работы, доходах с предыдущих мест работы;
- должность;
- размер заработной платы;
- сведения об открытых банковских счетах, на которые перечисляется заработная плата в ГБУ г. Москвы «ОКЦ СЗАО»:

- сведения о налоговых отчислениях и сборах;
- номер СНИЛС;
- ИНН;
- информация о приеме, переводе, увольнении и иных событиях, относящихся к моей трудовой деятельности в ГБУ г. Москвы «ОКЦ СЗАО»;
- сведения о доходах в ГБУ г. Москвы «ОКЦ СЗАО»;
- сведения о деловых и иных личных качествах, носящих оценочный характер.

Я не даю согласия на какое-либо распространение моих персональных данных и их передачу третьим лицам, включая физических и юридических лиц государственных органов и органов местного самоуправления, за исключением передачи персональных данных следующим организациям:

- Департамент информационных технологий города Москвы, в том числе подведомственные ему организации;
- Федеральная служба по труду и занятости;
- Социальный фонд России;
- Федеральная налоговая служба России;
- Префектура Северо-Западного административного округа города Москвы.

Обработка персональных данных должна осуществляться с соблюдением требований, установленных законодательством Российской Федерации и только для целей, указанных выше. ГБУ г. Москвы «ОКЦ СЗАО» обязано осуществлять защиту моих персональных данных, принимать необходимые организационные и технические меры для защиты моих персональных данных от неправомерного или случайного доступа к ним, уничтожения, модифицирования, блокирования, копирования, распространения, обезличивание, а также от иных неправомерных действий в отношении данной информации.

Обработка моих персональных данных для любых иных целей и любым иным способом, включая распространение и передачу их иным лицам, или иное их разглашение, может осуществляться только с моего письменного согласия в каждом отдельном случае.

Защита внесенной информации должна осуществляться с соблюдением требований, установленных законодательством Российской Федерации. Хранение и обработка информации, а также обмен информацией должны осуществляться после принятия необходимых мер по защите указанной информации. В случае нарушения требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» ГБУ г. Москвы «ОКЦ СЗАО» должно нести ответственность, предусмотренную Кодексом РФ об административных правонарушениях, Трудовым кодексом РФ, Уголовным кодексом РФ.

Данное согласие действует до достижения целей обработки персональных данных в ГБУ г. Москвы «ОКЦ СЗАО» или в течение срока хранения информации. Данное согласие может быть отозвано в любой момент по моему письменному заявлению в его части или полном объеме.

Я подтверждаю, что, давая настоящее согласие, я действую по своей воле и в своих интересах.

Дата: \_\_\_\_\_ г.

Подпись: \_\_\_\_\_ (\_\_\_\_\_)

Ф.И.О.

Приложение № 3  
к Положению по организации  
и проведению работ  
по обеспечению безопасности  
персональных данных  
при их обработке в Государственном  
бюджетном учреждении города  
Москвы «Объединение культурных  
и досуговых центров  
Северо-Западного  
административного округа»

### Форма акта об уничтожении персональных данных

«УТВЕРЖДАЮ»

\_\_\_\_\_ 202\_ г.  
« \_\_\_\_\_ » \_\_\_\_\_

Акт № \_\_\_\_\_  
об уничтожении персональных данных

№ п/п	Дата	Место и форма хранения персональных данных	Тип носителя персональных данных и его регистрационный номер/уничтожаемые персональные данные

Всего уничтожено носителей (прописью): \_\_\_\_\_

Уничтожение произведено путем

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_.

Ответственный за уничтожение (Ф.И.О., должность): \_\_\_\_\_.

Дата: \_\_\_\_\_.

Подпись: \_\_\_\_\_.