**ДЕПАРТАМЕНТ ОБРАЗОВАНИЯ И НАУКИ ГОРОДА МОСКВЫ**

**Государственное автономное учреждение города Москвы**
**«Медиацентр»**

# ПРИКАЗ

12.12.2024 № ПР-1Н-219/24

**Об утверждении документов, регулирующих обработку персональных данных в ГАУ Медиацентр**

В соответствии с Федеральным законом от 27.07.2006 № 152–ФЗ «О персональных данных», в целях реализации мер по обеспечению безопасности персональных данных в ГАУ Медиацентр

**приказываю:**

1. Назначить заместителя директора **О.В. Шорина** ответственным за организацию обработки персональных данных в ГАУ Медиацентр.

2. Назначить начальника отдела технического и системного сопровождения **Н.В. Новикова** ответственным за обеспечение безопасности персональных данных в ГАУ Медиацентр (далее – Ответственный) и возложить на него следующие обязанности:

2.1. Предоставление сведений о персональных данных в рамках проведения учета защищаемых носителей и проведения инвентаризации.

2.2. Установка, конфигурирование и администрирование аппаратных и программных средств защиты информации, применяемых для защиты персональных данных.

2.3. Учет защищаемых носителей персональных данных.

2.4. Учет технических средств защиты информации.

2.5. Проведение периодических проверок журналов безопасности.

2.6. Анализ защищенности информационных систем персональных данных.

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

2.8. Мониторинг порядка обработки персональных данных.

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

2.10. Выполнение иных задач, отнесенных локальными нормативными актами ГАУ Медиацентр к сфере деятельности Ответственного.

3. Утвердить документы, регулирующие обработку персональных данных в ГАУ Медиацентр:

3.1. Инструкцию пользователя по обеспечению безопасности персональных данных при их обработке в информационной системе согласно приложению № 1 к приказу;

3.2. Политику в отношении обработки персональных данных согласно приложению № 2 к приказу;

3.3. Положение об обработке персональных данных согласно приложению № 3 к приказу;

3.4. Положение по организации и проведению работ по обеспечению безопасности персональных данных при их обработке согласно приложению № 4 к приказу;

3.5. Порядок взаимодействия с уполномоченным органом по защите прав субъектов персональных данных приложению № 5 к приказу;

3.6. Порядок обработки обращений субъектов персональных данных согласно приложению № 6 к приказу;

3.7. Форму перечня сотрудников, допущенных до обработки персональных данных, согласно приложению № 7 к приказу;

3.8. Перечень персональных данных, обрабатываемых в ГАУ Медиацентр, согласно приложению № 8 к приказу;

3.9. Перечень персональных данных соискателей работы и лиц, претендующих на замещение вакантных должностей, обрабатываемых в ГАУ Медиацентр, согласно приложению № 9 к приказу;

3.10. Перечень персональных данных посетителей ГАУ Медиацентр согласно приложению № 10 к приказу;

3.11. Положение о режиме обеспечения безопасности помещений, в которых размещена информационная система, препятствующем возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения согласно приложению № 11 к приказу.

4. Признать утратившим силу приказ ГАОУ ДПО «ТемоЦентр» от 28.07.2021 № ПР–ЛН–15/21.

5. Контроль за исполнением приказа оставляю за собой.

**Директор**
**ГАУ Медиацентр** **В. А. Ловков**

Приложение № 1 к приказу ГАУ Медиацентр
от «12» 12 2024 г. № ПР-АН-219/24

# ИНСТРУКЦИЯ ПОЛЬЗОВАТЕЛЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННОЙ СИСТЕМЕ

## 1 Общие сведения

Инструкция пользователя по обеспечению безопасности персональных данных при их обработке в информационной системе (далее — Инструкция) устанавливает единый порядок обеспечения пользователями безопасности персональных данных и иной защищаемой информации при их обработке с использованием информационных систем и определяет:

– общие меры обеспечения безопасности информации и правила работы с информацией ограниченного доступа;

– правила по организации парольной защиты;

– правила по организации антивирусной защиты;

– правила по использованию съемных носителей;

– правила при работе с ресурсами сети Интернет и электронной почтой.

Инструкция обязательна для исполнения всеми пользователями информационных систем в Государственном автономном учреждении города Москвы «Медиацентр» (далее – ГАУ Медиацентр, Учреждение).

Пользователь должен ознакомиться с Инструкцией под роспись.

К защищаемой информации, обрабатываемой в ГАУ Медиацентр, относится информация ограниченного доступа – персональные данные работников и обучающихся, технологическая информация информационных систем, парольная информация.

К информационным системам, использующимся в Учреждении, относятся:

– информационные системы Правительства Москвы (в том числе Департамента образования и науки города Москвы и Департамента информационных технологий города Москвы, далее – централизованные ИС);

– локальные информационные системы Учреждения (далее – локальные ИС).

Допуск пользователей к работе в централизованных ИС осуществляется по заявке от руководства Учреждения и (или) ответственного за эксплуатацию системы. Допуск пользователей к работе в локальных ИС осуществляется в соответствии с должностными обязанностями пользователя.

## 2 Требования к уровню подготовки пользователя

Перед началом эксплуатации автоматизированного рабочего места пользователь должен ознакомиться:

– с положениями Инструкции;

– с регламентирующими документами по обеспечению информационной безопасности, принятыми в Учреждении;

– с руководствами по эксплуатации информационных систем, к которым пользователю предоставлен доступ.

Контроль знания требований нормативных документов по обеспечению информационной безопасности и Инструкции, а также контроль выполнения указанных требований возлагаются на ответственного за организацию обработки персональных данных в ГАУ Медиацентр (далее – Ответственный).

## 3 Обязанности пользователя

### 3.1 Общие положения

Пользователем информационной системы (далее – пользователь) является лицо, участвующее в процессах автоматизированной обработки информации в информационной системе и имеющее доступ к программному обеспечению и информации, обрабатываемой в этой системе.

Пользователь обязан:

– знать и соблюдать установленные Инструкцией правила обеспечения безопасности информации при работе с программными средствами и средствами защиты информации информационных систем согласно соответствующим инструкциям на данные средства;

– располагать во время работы экран видеомонитора в помещении таким образом, чтобы исключить возможность несанкционированного ознакомления с отображаемой на нем информацией посторонними лицами;

– обеспечить запирание помещения, в котором осуществляется работа с информационными системами при выходе всех работников из помещения;

– не отключать (блокировать) средства защиты информации;

– сообщать ответственному за эксплуатацию информационных систем о замеченных нарушениях информационной безопасности (в т. ч. о сбоях в работе средств защиты информации);

– при прекращении трудовых или гражданско–правовых отношений с Учреждением передать ответственному за организацию обработки персональных данных в Учреждении имеющиеся в пользовании материальные носители информации, содержащие информацию ограниченного доступа.

### 3.2 Правила работы с информацией ограниченного доступа

При работе с информацией ограниченного доступа пользователю запрещается:

– создавать и хранить документы, содержащие информацию ограниченного доступа, в папках, предназначенных для обмена открытыми документами;

– работать с информацией ограниченного доступа в общественных местах и на рабочих станциях, не оборудованных средствами защиты информации;

– осуществлять обработку информации на автоматизированном рабочем месте в присутствии лиц, не допущенных к данной информации;

– оставлять без личного контроля съемные и другие носители информации (в т. ч. и установленные на автоматизированном рабочем месте), распечатки, содержащие информацию ограниченного доступа;

– записывать на устройства, предназначенные для хранения информации ограниченного доступа, посторонние данные;

– использовать информацию ограниченного доступа в личных целях, в т. ч. в целях получения выгоды;

– выносить за пределы контролируемой зоны Учреждения материальные носители с информацией ограниченного доступа;

– оставлять без личного контроля включенное автоматизированное рабочее место без активированной блокировки.

### 3.3 Процедура блокирования доступа к автоматизированному рабочему месту

При необходимости временно прервать работу на автоматизированном рабочем месте для защиты от несанкционированного использования необходимо воспользоваться функцией временной блокировки компьютера, при которой блокируется клавиатура и экран монитора.

Порядок действий при блокировке автоматизированного рабочего места вручную: нажать комбинацию клавиш «Win» (между клавишами «Ctrl» и «Alt») + «L».

Для разблокировки автоматизированного рабочего места пользователю необходимо ввести свой пароль доступа.

### 3.4 Правила использования паролей

Пользователь должен следовать следующим правилам при использовании паролей, применяемых для доступа к автоматизированному рабочему месту и входу в информационные системы:

– использовать только свои персональные учетные записи (идентификаторы);

– хранить в тайне свой пароль (пароли), не размещать на рабочем месте документы, содержащие пароль (пароли), не передавать пароль (пароли) другим лицам;

– во время ввода пароля необходимо исключить возможность его просмотра посторонними лицами;

– не оставлять без присмотра автоматизированное рабочее место после ввода пароля.

Пользователь обязан использовать пароли, отвечающие следующим требованиям по парольной защите:

– длина пароля должна быть не менее 8 символов;

– в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т. п.);

– если информационная система позволяет изменять предустановленный (выданный администратором) пароль, то пользователь должен сменить пароль на новый при первом входе.

Выбранный пароль не должен поддаваться подбору, поэтому при выборе пароля запрещается:

– использовать в пароле имя пользователя (идентификатор) или его часть;

– использовать идущие подряд на клавиатуре и/или в алфавите символы (qwerty, 45678, abcdef);

– использовать распространенные осмысленные слова, общеупотребительные выражения или сокращения, имена собственные (USER, password, system, ADMIN, gftijkm («пароль» в английской раскладке);

– использовать три и более повторяющихся символов подряд (ggg254, UUU444).

При создании нового пароля необходимо обеспечить отличие вновь созданного пароля минимум на 1 символ от предыдущего. Запрещается использование последнего использованного пароля при создании нового пароля.

Пользователь обязан в случае подозрения на компрометацию пароля сообщить об этом ответственному за эксплуатацию соответствующей информационной системы и произвести смену пароля (самостоятельно, если такая функция доступна пользователю, либо совместно с ответственным).

### 3.5 Защита от воздействий вредоносных программ

Вредоносный код – любой программный код (компьютерный вирус, троян, сетевой червь), приводящий к нарушению функционирования средств вычислительной техники и/или предназначенный для искажения, модификации, уничтожения, блокирования или несанкционированного копирования информации. Вредоносный код способен создавать свои копии, сохраняющие все его свойства и требующие для своего размножения другие программы, каналы связи или машинные носители.

Возможен следующий характер проявлений действий вредоносного кода:

– искажение изображения на экране монитора;

– искажение символов, вводимых с клавиатуры;

– блокирование клавиатуры, звуковые эффекты;

– стирание или порча отдельных частей диска или файлов;

– повреждение загрузочных секторов жесткого диска персональной электронно–вычислительной машины и серверов;

– остановка загрузки или зависание компьютера, значительное замедление его работы;

– уничтожение или искажение информации о системной конфигурации персональной электронно–вычислительной машины и серверов.

В целях обеспечения защиты от воздействий вредоносного кода пользователю автоматизированного рабочего места запрещается:

– самостоятельно устанавливать программное обеспечение, в том числе командные файлы;

– использовать при работе «зараженный» вредоносным кодом либо с подозрением на «заражение» носитель информации и/или файл;

– использовать личные носители информации на автоматизированном рабочем месте;

– использовать служебные носители информации на домашних компьютерах и в неслужебных целях;

– самостоятельно отключать, удалять и изменять настройки установленных средств защиты информации.

Пользователь автоматизированного рабочего места обязан проводить контроль на отсутствие вредоносных программ любых сменных и подключаемых носителей (дискет, CD–дисков, DVD–дисков, Flash–памяти) и открываемых архивов (ZIP. RAR и др.).

### 3.6 Правила обращения со съемными носителями

Пользователь вправе использовать съемные носители информации только в случаях, когда это необходимо для выполнения трудовых (служебных) обязанностей. При использовании таких носителей пользователь обязан:

– использовать их исключительно для выполнения трудовых обязанностей и не использовать в личных целях;

– обеспечивать их физическую безопасность;

– обеспечивать проверку отсутствия на них вредоносного программного обеспечения;

– извещать Ответственного за организацию обработки персональных данных в Учреждении о фактах утери съемных носителей, содержавших персональные данные работников и (или) обучающихся;

– не передавать съемные носители третьим лицам при отсутствии в этом производственной необходимости;

– не оставлять съемные носители без присмотра.

### 3.7 Использование электронной почты и ресурсов сети Интернет

При использовании электронной почты пользователям запрещается:

– пересылать информацию ограниченного доступа с использованием общедоступных почтовых сервисов (Яндекс, Рамблер, Mail.ru, Google и другие);

– открывать вложения подозрительных электронных сообщений (сообщений от незнакомых отправителей, сообщений, содержащих исполняемые файлы (EXE, COM, BAT); сообщений рекламного, развлекательного, оскорбительного характера);

– переходить по ссылкам на сайты из подозрительных электронных сообщений, в том числе сообщений, содержащих приглашения «открыть», «запустить», «посетить», «нажать», «перейти»;

– отправлять электронные письма от имени других работников Учреждения, если иное не определено их служебными обязанностями;

– предпринимать попытки несанкционированного доступа к почтовым ящикам других работников Учреждения.

При использовании ресурсов сети Интернет–пользователям запрещается:

– использовать для обмена информацией ограниченного доступа сайты, предоставляющие услуги хранения и обмена информацией;

– размещать, публиковать информацию ограниченного доступа на общедоступных ресурсах;

– загружать из сети Интернет программное обеспечение и устанавливать его на автоматизированные рабочие места;

– предпринимать попытки к получению несанкционированного доступа к ресурсам сети Интернет, в том числе использовать специализированные средства для обхода блокировок ресурсов, установленных поставщиком услуг связи, Департаментом информационных технологий города Москвы и/или инженером по автоматизации (техником) Учреждения.

### 3.8 Порядок действий в случае возникновения нештатных ситуаций

В случае возникновения нештатных ситуаций (инцидентов) пользователь обязан обратиться с описанием проблемы к инженеру по автоматизации (технику), ответственному за эксплуатацию соответствующей информационной системы в Учреждении и при необходимости – в службу технической поддержки информационной системы при возникновении нештатных ситуаций, связанных с использованием информационных систем, а также в случаях:

– подозрения на компрометацию (утерю, разглашение, несанкционированное копирование или использование) личных паролей;

– подозрения на наличие вредоносных программ (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т. п.);

– обнаружения фактов совершения в отсутствие пользователя попыток несанкционированного доступа к техническим средствам и носителям информации (следов вскрытия, измененного состава подключенных устройств, кабелей, в том числе отводов кабелей);

– невозможности запуска средств защиты информации или при ошибках в процессе их выполнения;

– несанкционированных изменений в конфигурации программного обеспечения;

– отклонений в нормальной работе программного обеспечения, затрудняющих эксплуатацию автоматизированного рабочего места;

– обнаружения ошибок в программном обеспечении.

## 4 Ответственность пользователя

Пользователь несет персональную ответственность за надлежащее исполнение своих обязанностей, а также сохранность технических средств автоматизированного рабочего места, съемных носителей информации, электронных идентификаторов и целостность установленного программного обеспечения.

Пользователи, виновные в нарушениях требований Инструкции, несут уголовную, административную, гражданско–правовую или дисциплинарную ответственность в соответствии с законодательством Российской Федерации.

Приложение № 2 к приказу ГАУ Медиацентр
от «12» 12 2024 г. №ПР-ЛН-219/24

# ПОЛИТИКА В ОТНОШЕНИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

## 1. Введение

1.1 Политика в отношении обработки персональных данных (далее – Политика) разработана в соответствии с Федеральным законом от 27.07.2006 № 152–ФЗ «О персональных данных» (далее – Закон о 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 Государственное автономное учреждение города Москвы «Медиацентр» (далее – Учреждение) является оператором персональных данных в соответствии с законодательством Российской Федерации о персональных данных.

1.3 Действие Политики распространяется на любое действие (операцию) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств, с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

1.4 Политика подлежит актуализации в случае изменений законодательства Российской Федерации о персональных данных.

## 2 Принципы обработки персональных данных

Обработка персональных данных осуществляется на основе следующих принципов:

1) обработка персональных данных осуществляется на законной и справедливой основе;

2) обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей;

3) обработка персональных данных, несовместимая с целями сбора персональных данных, не допускается;

4) не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;

5) содержание и объем обрабатываемых персональных данных соответствуют заявленным целям обработки. Обрабатываемые персональные данные не являются избыточными по отношению к заявленным целям обработки;

6) при обработке персональных данных обеспечивается точность персональных данных и их достаточность (в случаях необходимости) и актуальность персональных данных по отношению к заявленным целям их обработки;

7) хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не

установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных;

8) обрабатываемые персональные данные подлежат уничтожению или обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

## 3 Условия обработки персональных данных

3.1 Обработка персональных данных осуществляется с соблюдением принципов и правил, установленных Законом о персональных данных. Обработка персональных данных осуществляется в следующих случаях:

3.1.1 Обработка персональных данных осуществляется с согласия субъекта персональных данных или его законного представителя на обработку его персональных данных.

3.1.2 Обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей.

3.1.3 Обработка персональных данных осуществляется в связи с участием лица в конституционном, гражданском, административном, уголовном судопроизводстве, судопроизводстве в арбитражных судах.

3.1.4 Обработка персональных данных необходима для исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве.

3.1.5 Обработка персональных данных необходима для исполнения полномочий федеральных органов исполнительной власти, органов государственных внебюджетных фондов, исполнительных органов государственной власти г. Москвы, органов местного самоуправления и функций организаций, участвующих в предоставлении государственных и муниципальных услуг, предусмотренных Федеральным законом от 27.07.2010 № 210–ФЗ «Об организации предоставления государственных и муниципальных услуг».

3.1.6 Обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем.

3.1.7 Обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно.

3.1.8 Обработка персональных данных необходима для осуществления прав и законных интересов оператора или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта

персональных данных.

3.1.9 обработка персональных данных необходима для осуществления профессиональной деятельности журналиста и (или) законной деятельности средства массовой информации либо научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и законные интересы субъекта персональных данных.

3.1.10 Обработка персональных данных осуществляется в статистических или иных исследовательских целях (за исключением целей обработки в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи) при условии обязательного обезличивания персональных данных.

3.1.11 Обработка персональных данных, полученных в результате обезличивания персональных данных, осуществляется в целях повышения эффективности государственного или муниципального управления, а также в иных целях, предусмотренных Федеральным законом от 24.04.2020 № 123–ФЗ «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации – городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных» и Федеральным законом от31.07.2020 № 258–ФЗ «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации», в порядке и на условиях, которые предусмотрены указанными федеральными законами.

3.1.12 Осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом, в частности, с нормами информационной открытости Учреждения согласно Федеральному закону от 29.12.2012 № 273–ФЗ «Об образовании в Российской Федерации».

3.2 Учреждение может включать персональные данные субъектов в общедоступные источники персональных данных, при этом Учреждение берет письменное согласие субъекта на обработку его персональных данных.

3.3 Учреждение может осуществлять обработку данных о состоянии здоровья субъекта персональных данных:

3.3.1 В случаях, предусмотренных законодательством о государственной социальной помощи, трудовым законодательством, пенсионным законодательством Российской Федерации.

3.3.2 В медико–профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико–социальных услуг, при наличии в штате Учреждения лица, профессионально занимающегося медицинской деятельностью и обязанного в соответствии с законодательством Российской Федерации сохранять врачебную тайну.

3.3.3 В целях защиты жизни, здоровья или иных жизненно важных интересов работника либо для защиты жизни, здоровья или иных жизненно важных интересов

других лиц и получение согласия субъекта персональных данных невозможно.

3.3.4 В целях установления или осуществления прав субъекта персональных данных или третьих лиц, а равно и в связи с осуществлением правосудия.

3.3.5 В случаях, предусмотренных законодательством об обязательных видах страхования, страховым законодательством, об обороне, о противодействии коррупции и иным специальным законодательством.

3.4 В Учреждении не обрабатываются биометрические персональные данные (сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных), за исключением фотографий.

3.5 Учреждение не осуществляет трансграничную передачу персональных данных.

3.6 Принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы, не осуществляется.

3.7 При отсутствии необходимости письменного согласия субъекта на обработку его персональных данных согласие субъекта может быть дано субъектом персональных данных или его законным представителем в любой позволяющей получить факт его получения форме.

3.8 Учреждение вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора (далее – поручение оператора). При этом Учреждение в поручении оператора обязует лицо, осуществляющее обработку персональных данных по поручению Учреждения, соблюдать принципы и правила обработки персональных данных, предусмотренные Законом о персональных данных.

3.9 В случае, если Учреждение поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет Учреждение. Лицо, осуществляющее обработку персональных данных по поручению Учреждения, несет ответственность перед Учреждением.

## 4 Обязанности Учреждения

В соответствии с требованиями Закона о персональных данных Учреждение обязано:

4.1 Предоставлять субъекту персональных данных по его запросу информацию, касающуюся обработки его персональных данных, либо на законных основаниях предоставить отказ в течение тридцати дней с даты получения запроса субъекта персональных данных или его представителя.

4.2 По требованию субъекта персональных данных уточнять, блокировать или удалять обрабатываемые персональные данные, если персональные данные

являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, в срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих эти факты.

4.3 Вести журнал учета обращений субъектов персональных данных, в котором должны фиксироваться запросы субъектов персональных данных на получение персональных данных, а также факты предоставления персональных данных по этим запросам.

4.4 Уведомлять субъекта персональных данных об обработке персональных данных в том случае, если персональные данные были получены не от субъекта персональных данных. Исключение составляют следующие случаи:

4.4.1. Субъект персональных данных уведомлен об осуществлении обработки Учреждением его персональных данных.

4.4.2. Персональные данные получены Учреждением в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, или на основании федерального закона.

4.4.3. Персональные данные сделаны общедоступными субъектом персональных данных или получены из общедоступного источника.

4.4.4. Учреждение осуществляет обработку персональных данных для статистических или иных исследовательских целей, если при этом не нарушаются права и законные интересы субъекта персональных данных.

4.4.5. Предоставление субъекту персональных данных сведений, содержащихся в уведомлении об обработке персональных данных, нарушает права и законные интересы третьих лиц.

4.5 В случае достижения цели обработки персональных данных незамедлительно прекратить обработку персональных данных и уничтожить соответствующие персональные данные в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между Учреждением и субъектом персональных данных, либо если Учреждение не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Законом о персональных данных или другими федеральными законами.

4.6 В случае отзыва субъектом персональных данных согласия на обработку своих персональных данных прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено соглашением между Учреждением и субъектом персональных данных.
Об уничтожении персональных данных Учреждение обязано уведомить субъекта персональных данных.

4.7 В случае поступления требования субъекта персональных данных о

прекращении обработки персональных данных, полученных в целях продвижения товаров, работ, услуг на рынке, немедленно прекратить обработку персональных данных.

4.8 Учреждение обязуется и обязует иные лица, получившие доступ к персональным данным, не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

## 5 Меры по обеспечению безопасности персональных данных при их обработке

5.1 При обработке персональных данных Учреждение применяет необходимые правовые, организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

5.2 Обеспечение безопасности персональных данных достигается, в частности:

5.2.1 Определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

5.2.2 Применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных.

5.2.3 Применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации.

5.2.4 Оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных.

5.2.5 Учетом машинных носителей персональных данных.

5.2.6 Обнаружением фактов несанкционированного доступа к персональным данным и принятием мер.

5.2.7 Восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

5.2.8 Установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональных данных в информационной системе персональных данных.

5.2.9 Контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

## 6 Права субъекта персональных данных

В соответствии с Законом о персональных данных субъект персональных данных имеет право:

6.1 Получить сведения, касающиеся обработки персональных данных Учреждением, а именно:

6.1.1. Подтверждение факта обработки персональных данных Учреждением.

6.1.2. Правовые основания и цели обработки персональных данных Учреждением.

6.1.3. Применяемые Учреждением способы обработки персональных данных.

6.1.4. Наименование и место нахождения Учреждения, сведения о лицах, которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона.

6.1.5. Обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом.

6.1.6. Сроки обработки персональных данных Учреждением, в том числе сроки их хранения.

6.1.7. Порядок осуществления субъектом персональных данных прав, предусмотренных Законом о персональных данных.

6.1.8. Информацию об осуществленной или предполагаемой трансграничной передаче данных.

6.1.9. Наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Учреждения, если обработка поручена или будет поручена такому лицу.

6.1.10. Иные сведения, предусмотренные Законом о персональных данных или другими федеральными законами.

6.2 Потребовать от Учреждения уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки.

6.3 Отозвать согласие на обработку персональных данных в предусмотренных законом случаях.

6.4 Принять предусмотренные законом меры по защите своих прав.

## 7 Порядок осуществления прав субъекта персональных данных

7.1 Обращение субъекта персональных данных к оператору в целях реализации его прав, установленных Законом о персональных данных, осуществляется в письменном виде либо при личном визите в Учреждение субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

7.2 Форма обращения выдается субъекту персональных данных или его представителю ответственным за обработку персональных данных лицом (или

секретарем Учреждения) и заполняется субъектом персональных данных или его представителем с проставлением собственноручной подписи в присутствии ответственного за обработку персональных данных лица.

7.3 Ответственный за обработку персональных данных (или секретарь), получив обращение по установленной форме, сверяет указанные в нем сведения об основном документе, удостоверяющем личность субъекта персональных данных, основания, по которым лицо выступает в качестве представителя субъекта персональных данных, и представленные при обращении оригиналы данного документа.

7.4 Ответ на обращение отправляется субъекту персональных данных в письменном виде по почте на адрес, указанный в обращении.

7.5 Срок формирования ответа и его передачи в почтовое отделение для отправки не может превышать тридцати дней с даты получения Учреждением соответствующего обращения.

7.6 Срок внесения необходимых изменений в персональные данные, являющиеся неполными, неточными или неактуальными, не может превышать семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными.

7.7 Срок уничтожения персональных данных, являющихся незаконно полученными или не являющихся необходимыми для заявленной цели обработки, не может превышать десяти рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки.

## 8 Ограничения прав субъектов персональных данных

8.1 Право субъекта персональных данных на доступ к своим персональным данным ограничивается в случае, если предоставление персональных данных нарушает права и законные интересы других лиц.

8.2 В случае, если сведения, касающиеся обработки персональных данных, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе направить повторный запрос в целях получения сведений, касающихся обработки персональных данных, и ознакомления с такими персональными данными не ранее чем через тридцать дней после направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

8.3 Субъект персональных данных вправе направить Учреждению мотивированный повторный запрос в целях получения сведений, касающихся обработки персональных данных, а также в целях ознакомления с обрабатываемыми

персональными данными до истечения срока, указанного в пункте 8.2 Политики, в случае, если такие сведения и/или обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального запроса.