УТВЕРЖДЕНО
приказом ГКУ «ЦБДДМО»
от 28.01.2020 № 10

ПОЛОЖЕНИЕ
ГКУ «ЦБДДМО» о защите и обработке персональных данных

Перечень используемых сокращений

Сокращение	Полное наименование
ИСПДн	Информационная система персональных данных
Учреждение	Государственное казенное учреждение Московской области «Центр безопасности дорожного движения»
ПДн	Персональные данные
Роскомнадзор	Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций
СЗПДн	Система защиты персональных данных
ФСТЭК России	Федеральная служба по техническому и экспортному контролю России
ФСБ России	Федеральная служба безопасности России

Перечень терминов и определений

Термин	Определение
Информационная система персональных данных	Совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств
Обезличивание персональных данных	Действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных
Обработка персональных данных	Любое действие (операция) 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
Оператор	Государственное казенное учреждение Московской области «Центр безопасности дорожного движения» (далее – Учреждение), самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными

Персональные данные	Любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)
Уничтожение персональных данных	Действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных

I. Общие положения

ГКУ «ЦБДДМО» (далее – Учреждение) является оператором персональных данных. В соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», на операторов персональных данных возлагается ответственность за защиту обрабатываемых персональных данных.

Настоящее Положение устанавливает порядок обработки персональных данных (далее — Положение) и действует в отношении всех персональных данных, которые ГКУ «ЦБДДМО» может получить от субъектов персональных данных.

Обработка ПДн в Учреждении включает сбор, систематизацию, накопление, хранение, изменение, использование, передачу, обезличивание, блокирование и уничтожение ПДн.

Целью данного Положения является формирование общих подходов к обеспечению информационной безопасности ПДн, обрабатываемых в Учреждении.

Обработка ПДн в Учреждении осуществляется в целях обеспечения соблюдения Конституции Российской Федерации, федеральных законов и иных нормативных правовых актов Российской Федерации, содействия работнику в трудоустройстве, обучении, получении образования и продвижении по службе, учете результатов исполнения работником должностных обязанностей, обеспечении работнику установленных законодательством Российской Федерации условий труда, гарантий и компенсаций, сохранности принадлежащего ему имущества и имущества Учреждения, а также ведения кадрового документооборота.

Обработка ПДн в Учреждении осуществляется как с применением средств автоматизации, так и без использования таковых.

Условием прекращения обработки ПДн в Учреждении является ликвидация или реорганизация Учреждения.

ПДн обрабатываются в Учреждении в минимальном объеме и составе,

необходимом для достижения заявленных целей, и не дольше, чем этого требуют цели их обработки.

Обработка и защита ПДн работников Учреждения осуществляется в соответствии с настоящим Положением.

Настоящее Положение устанавливает:

основные направления обеспечения информационной безопасности ПДн;

ограничения на порядок обработки ПДн для обеспечения их безопасности;

ответственность за защиту ПДн в Учреждении.

Положение о защите ПДн разработано на основании требований:

Конституции Российской Федерации;

Трудового Кодекса Российской Федерации;

Федерального Закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

Федерального Закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

постановления Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

постановления Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

приказа ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

иных нормативных и правовых актов Российской Федерации и нормативных документов Учреждения.

Настоящее Положение вступает в силу с момента подписания приказа об утверждении настоящего Положения директором Учреждения.

Пересмотр Положения производится:

планово (не реже одного раза в год);

внепланово (при изменении действующего законодательства, нормативно-методической документации Учреждения, и т.д.).

Все изменения в Положение утверждаются приказом.

Требования данного документа распространяются на работников Учреждения.

Работники должны быть ознакомлены с настоящим Положением под роспись.

II. Основные меры по защите персональных данных

В целях предотвращения и нейтрализации угроз безопасности ПДн

в Учреждении применяются следующие меры защиты:

правовые;

организационные;

технические.

Правовые меры предусматривают организацию работ по защите ПДн, разработку внутренних нормативно-технических и организационно-распорядительных документов, регламентирующих вопросы защиты ПДн и отвечающих требованиям нормативных документов по защите ПДн.

Организационные меры обеспечения информационной безопасности предусматривают:

ознакомление работников с правилами обработки и защиты ПДн;

установление ответственности работников Учреждения за выполнение назначенных требований по защите ПДн;

контроль за соблюдением работниками требований по защите ПДн;

обучение пользователей ИСПДн и персонала, обслуживающего СЗПДн;

проведение анализа эффективности и достаточности принятых мер по защите ПДн, обрабатываемых как с использованием средств автоматизации, так и без таковых.

Технические меры обеспечения информационно безопасности предусматривают:

внедрение, эксплуатацию, совершенствование СЗПДн и оценку эффективности защиты ИСПДн;

использование средств защиты, соответствующих задаваемым требованиям по безопасности ПДн.

III. Основные направления работ по защите персональных данных

Учреждение обеспечивает защиту ПДн, обрабатываемых в Учреждении, как с использованием средств автоматизации, так и без использования таких средств.

Основными направления работ по обеспечению безопасности ПДн являются:

организация деятельности по обеспечению безопасности ПДн;

формирование Перечня ПДн;

обследование информационных ресурсов на предмет наличия в них ПДн;

установление ограничений на порядок обработки ПДн;

организация разрешительной системы доступа работников к обработке ПДн;

организация и проведение работ по обеспечению безопасности ПДн при их обработке в ИСПДн;

контроль соблюдения мер по защите ПДн при их обработке.

IV. Организация деятельности по обеспечению безопасности персональных данных

Организация и управление деятельностью по обеспечению безопасности ПДн в Учреждении осуществляется директором Учреждения.

Приказом директора в Учреждении создается постоянно действующая рабочая группа по организации работ по защите ПДн (далее – Рабочая группа).

План работы Рабочей группы утверждается директором Учреждения.

На Рабочую группу возлагаются обязанности по разработке и организации мероприятий по защите ПДн.

Для защиты ПДн при их обработке в Учреждении применяются следующие организационные и технические меры:

доступ к ПДн предоставляется только тем работникам Учреждения, на которых возложена обязанность по их обработке. Указанные лица имеют право на обработку только тех персональных данных, которые необходимы им для выполнения конкретных функций, связанных с исполнением должностных обязанностей;

обработка ПДн ведется работниками Учреждения на рабочих местах, выделенных для исполнения ими должностных обязанностей;

рабочие места размещаются таким образом, чтобы исключить бесконтрольное использование конфиденциальной информации;

конфиденциальная информация, содержащая персональные данные субъектов ПДн, проходит процедуру уничтожения в сроки, установленные законодательством Российской Федерации;

проводятся процедуры, направленные на обнаружение фактов несанкционированного доступа к ПДн и принятие соответствующих мер;

разграничены права доступа к ПДн, обрабатываемым в информационных системах персональных данных;

проводится ознакомление работников Учреждения, непосредственно осуществляющих обработку ПДн либо имеющих к ним доступ в силу своих должностных обязанностей, с положениями законодательства Российской Федерации, требованиями к защите персональных данных, локальными нормативными актами Учреждения по вопросам обработки персональных данных;

своевременно выявляются и предотвращаются нарушения требований законодательства Российской Федерации в области обработки персональных данных, устраняются последствия таких нарушений;

проводится контроль за принимаемыми мерами по обеспечению безопасности персональных данных при их обработке, а также проводится контроль соответствия обработки персональных данных требованиям Федерального закона «О персональных данных» от 27.07.2006 № 152-ФЗ и принятым в соответствии

с ним нормативным правовым актам, требованиям к защите персональных данных, локальным нормативным актам Учреждения.

V. Формирование перечня персональных данных

Перечень ПДн, обрабатываемых в Учреждении (как с использованием средств автоматизации, так и без использования таких средств) (далее – Перечень) с указанием целей, способов и сроков обработки таких данных формируется Рабочей группой и утверждается директором Учреждения. Данный Перечень формируется на основе перечней ПДн, обрабатываемых в структурных подразделениях Учреждения. Перечень составляется в бумажной либо электронной форме (Приложение 2).

В Перечень необходимо включать любые сведения, позволяющие идентифицировать субъекта ПДн, в том числе:

анкетные и биографические данные;

образование;

сведения о составе семьи;

паспортные данные;

сведения о воинском учете;

сведения о заработной плате работника;

сведения о социальных льготах;

специальность;

занимаемая должность;

наличие судимостей;

адрес места жительства;

личный мобильный и домашний телефон;

содержание трудового договора;

трудовая книжка или сведения о трудовой деятельности;

дела, содержащие материалы по повышению квалификации и переподготовке работников, их аттестации, служебным расследованиям;

прочие сведения, которые могут идентифицировать субъект ПДн.

В целях определения необходимого объема, состава ПДн, целей, сроков и способов их обработки в структурном подразделении Учреждения его руководителем создается рабочая группа либо назначаются ответственные за предоставление данных.

При формировании перечня ПДн, обрабатываемых в структурном подразделении Учреждения, Рабочая группа руководствуется следующими принципами:

цели обработки ПДн в подразделении должны соответствовать задачам,

решаемым этим подразделением;

объем, состав, срок и способ обработки ПДн должны соответствовать целям их обработки.

В случае выявления Рабочей группой превышения необходимого объема и состава ПДн, обрабатываемых в структурном подразделении, формируются предложения по сокращению объема и состава обрабатываемых данных.

Предложения рассматриваются руководителями структурных подразделений и (при необходимости) директором Учреждения. По результатам рассмотрения выносится решение об изменении/не изменении объема и состава обрабатываемых данных.

Пересмотр Перечня выполняется раз в год или по необходимости (в случае изменения организационной структуры Учреждения и т.д.).

VI. Обследование информационных ресурсов на предмет наличия в них персональных данных

С целью выявления наличия в информационных ресурсах Учреждения ПДн для дальнейшей их защиты выполняется обследование информационных ресурсов. Организация данной деятельности возлагается на Рабочую группу.

Обследованию подлежат все информационные ресурсы Учреждения.

Обследование информационных ресурсов осуществляется с помощью:

анализа формализованных описаний процессов автоматизированной обработки информации в корпоративных информационных системах;

анализа утвержденных документов, регламентирующих выполнение функциональных задач пользователями Учреждения (Инструкций, Положений, Регламентов и т.д.);

интервьюирования работников.

Информация об информационных ресурсах, содержащих ПДн, вносится в Перечень информационных ресурсов, содержащих ПДн Учреждения. Перечень составляется в бумажной либо электронной форме (Приложение 3).

Пересмотр Перечня информационных ресурсов, содержащих ПДн Учреждения, выполняется раз в год или по необходимости (при появлении новых информационных ресурсов, содержащих ПДн; прекращении обработки ПДн в существующих информационных ресурсах).

VII. Установление ограничений на порядок обработки персональных данных

На действия с ПДн накладываются ограничения, устанавливающие особый

порядок обработки ПДн. Данные ограничения касаются следующих областей деятельности:

получение ПДн;

хранение ПДн;

организация работы с документами и другими материальными носителями, содержащими ПДн;

принятие решений в отношении субъекта ПДн;

организация работы с обращениями субъектов ПДн;

организация разрешительной системы доступа к ПДн.

Обработка ПДн осуществляется Учреждением с согласия субъектов ПДн, за исключением установленных законодательством случаев.

ПДн могут быть получены:

непосредственно у субъекта ПДн;

у третьей стороны, имеющей право передавать ПДн субъекта (получившей письменное согласие субъекта на передачу его данных третьим лицам).

В случаях, когда Учреждение получает ПДн у третьей стороны, субъект ПДн уведомляется о факте обработки его ПДн в Учреждении. Обработка ПДн в указанном случае осуществляется с письменного согласия субъекта ПДн.

Согласия субъекта на получение его ПДн от третьей стороны и уведомления о факте обработки не требуется в случаях, когда согласие субъекта на передачу его ПДн Учреждение получено третьей стороной.

Хранение ПДн в Учреждении осуществляется в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели их обработки. По достижению целей обработки или в случае утраты необходимости в их достижении, ПДн подлежат уничтожению.

В случае необходимости продолжения обработки ПДн в статистических и иных целях, ПДн обезличиваются. Мероприятия по разработке механизмов обезличивания включаются в План мероприятий по защите ПДн.

При хранении ПДн работниками Учреждения принимаются необходимые организационные и технические меры для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения ПДн, и иных неправомерных действий.

На процедуры обработки ПДн накладываются ограничения в соответствии с постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

В Учреждении принятие решений в отношении субъектов ПДн осуществляется исключительно при непосредственном участии человека в их обработке.

В соответствии с Федеральным Законом от 27 июля 2006 г. № 152-ФЗ

«О персональных данных» на Учреждение, как оператора ПДн, возлагается обязанность своевременно реагировать на обращения и запросы субъектов ПДн. В связи с этим в Учреждении организуется деятельность по работе с обращениями и запросами субъектов ПДн. Мероприятия по организации данной деятельности вносятся в План мероприятий по защите ПДн (Приложение 1).

VIII. Организация разрешительной системы доступа работников к обработке персональных данных

Защита ПДн в Учреждении предусматривает организацию разрешительной системы доступа работников к обработке ПДн.

В рамках организации разрешительной системы доступа работниками отдела информационных технологий, на основании предложений руководителей структурных подразделений в бумажной либо электронной форме формируется Список работников, обрабатывающих ПДн (Приложение 4).

Данный список утверждается директором Учреждения.

При формировании предложений по составу работников, допущенных к обработке ПДн, учитываются функциональные обязанности работников.

Список работников, обрабатывающих ПДн, пересматривается по мере необходимости, но не реже одного раза в год.

При приеме на работу в Учреждение (изменении должностных обязанностей) работники, должностные обязанности которых включают участие в обработке ПДн, обязаны взять на себя обязательства о неразглашении сведений, составляющих ПДн.

Доступ к ПДн предоставляется в объемах, необходимых для выполнения конкретных функций и трудовых обязанностей, в соответствии с утвержденным Списком работников, обрабатывающих ПДн.

Доступ работников к обработке ПДн прекращается в случаях:

нарушения работником режима конфиденциальности ПДн;

изменения должностных обязанностей работника (в том случае если новые должностные обязанности не требуют доступа к обработке ПДн);

увольнения работника.

При прекращении доступа к ПДн работник не освобождается от принятых им обязательств по неразглашению ПДн.

Право доступа к ПДн которые необходимы для выполнения определенных задач, без специального разрешения имеют работники, занимающие следующие должности:

- директор;
- первый заместитель директора;
- заместители директора;

- главный бухгалтер;
- работники отдела бухгалтерского учета и отчетности;
- работники отдела кадров и режима;
- работники общего отдела;
- работники отдела информационных технологий;
- работники юридического отдела;
- работники отдела организации помощи при ДТП (доступ к ПДн только в рамках исполнения своих должностных обязанностей);
- начальники структурных подразделений (доступ к ПДн только работников своего подразделения).

IX. Организация и проведение работ по обеспечению безопасности персональных данных при их обработке

Работы по обеспечению безопасности ПДн при их обработке в ИСПДн являются неотъемлемой частью действий по созданию информационных систем, а также включаются Рабочей группой в план мероприятий и состоят из следующих этапов:

определение типа угроз безопасности ПДн, актуальных для информационной системы;

установление уровня защищенности ПДн и его документальное оформление;

формирование требований к СЗПДн;

реализация требований по защите ПДн в ИСПДн;

разработка комплекта организационно-распорядительных и эксплуатационно-технических документов по вопросам обеспечения информационной безопасности ПДн, обеспечения функционирования и использования технических средств системы защиты ПДн.

Разработка частной модели угроз безопасности, а также установление уровня защищенности ПДн, выполняются в соответствии с постановлениями Правительства Российской Федерации нормативными правовыми актами ФСТЭК России, Роскомнадзора и ФСБ России.

Для каждой из ИСПДн в зависимости от уровней защищенности и актуальных угроз устанавливаются необходимые требования к защите ПДн.

На основании сформированных требований создается СЗПДн, включающая организационные меры и технические средства защиты информации.

Вне зависимости от определенного уровня защищенности ИСПДн для защиты информации в них применяются технические и программные средства, удовлетворяющие установленным в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

На стадии ввода в действие ИСПДн (СЗПДн) проводится оценка эффективности

мер по обеспечению безопасности ПДн.

Пересмотр результатов оценки эффективности, анализа угроз безопасности, определения уровня защищенности проводится не реже одного раза в 3 года или по необходимости.

X. Контроль соблюдения мер по защите персональных данных при их обработке

С целью определения соответствия принятых мер по защите ПДн положениям настоящего документа, выявления возможных каналов утечки и несанкционированного доступа к таким данным и принятию мер по их пресечению, в Учреждении осуществляется контроль исполнения требований по защите ПДн.

Контроль заключается в проверке выполнения требований нормативных и организационно-распорядительных документов по защите ПДн, а также в оценке обоснованности и эффективности принятых мер, и предполагает проверку эффективности, как организационных, так и технических мероприятий по защите ПДн.

Контроль исполнения требований по защите ПДн осуществляется в виде:

постоянного мониторинга информационной безопасности ПДн;

периодической оценки эффективности реализованных мер по обеспечению информационной безопасности ПДн.

Постоянный мониторинг проводится в целях:

оперативного выявления удавшихся и неудавшихся попыток нарушения безопасности ПДн;

обнаружения событий, служащих признаками возникновения инцидентов безопасности ПДн, и позволяющих предотвращать эти инциденты;

реагирования на действия и события, которые могли бы оказать воздействие на эффективность системы защиты ПДн;

обновления плана мероприятий по защите ПДн с учетом результатов постоянного мониторинга.

Постоянный мониторинг информационной безопасности ПДн осуществляется путем:

контроля соблюдения работниками Учреждения организационных мер;

безопасности при работе с материалами, содержащими ПДн (осуществляется руководителями структурных подразделений);

контроля защищенности ПДн, обрабатываемых в автоматизированных системах (осуществляется работниками отдела информационных технологий);

контроля защищенности ПДн, передаваемых по каналам (сетям, системам) связи (осуществляется работниками отдела информационных

технологий).

Периодическая оценка эффективности проводится в целях:

определения соответствия принимаемых мер по обеспечению безопасности ПДн, установленным требованиям нормативных документов по защите ПДн;

проверки эффективности мер по защите ПДн;

обновления плана мероприятий по защите ПДн с учетом результатов периодической оценки эффективности.

Оценка эффективности осуществляется путем:

внутреннего аудита состояния информационной безопасности ПДн, обрабатываемых в ИСПДн (проводится Учреждением самостоятельно);

внешнего аудита состояния информационной безопасности ПДн, обрабатываемых в ИСПДн (проводится внешними, независимыми организациями-аудиторами при необходимости).

Объектом контроля при проведении как внешнего, так и внутреннего аудита состояния информационной безопасности ПДн, обрабатываемых в ИСПДн, является совокупность следующих элементов:

помещения, в которых производится обработка ПДн;

организационно-распорядительные, эксплуатационно-технические документы, регламентирующие вопросы обеспечения информационной безопасности ПДн, обеспечения функционирования и использования технических средств СЗПДн;

деятельность работников Учреждения, участвующих в обработке ПДн;

комплексы и программно-технические элементы, на которых осуществляется обработка ПДн.

В целях осуществления периодической оценки эффективности мер по обеспечению информационной безопасности ПДн Учреждения разрабатывается план внутренних проверок состояния защиты ПДн (далее – План проверок), на основании которого проводится внутренний и внешний аудит.

Аудит состояния информационной безопасности ПДн проводится не реже одного раза в три года. Для проведения аудита создается проверяющая комиссия. Предложения по составу проверяющей комиссии подготавливаются Рабочей группой, при этом в нее в обязательном порядке должны входить представители отдела информационных технологий. Состав проверяющей комиссии утверждается приказом директора Учреждения.

При проведении внешнего аудита функциями вышеперечисленных работников является осуществление контроля за ходом проведения проверок и оказание информационной поддержки лицам, участвующим в проведении проверок.

В ходе проверок в обязательном порядке принимаются меры по ограничению необоснованного раскрытия ПДн лицам, участвующим в проведении проверок.

При выявлении в ходе проверки недостатков и нарушений, проверяющая

комиссия устанавливает сроки и ответственных за устранение данных недостатков и нарушений. Результаты устранения контролируются членами проверяющей комиссии.

XI. Обеспечение безопасности персональных данных при взаимодействии с субъектами персональных данных

При взаимодействии с субъектами ПДн Учреждения обеспечивается соблюдение их прав в соответствии с законодательством Российской Федерации.

В соответствии с Федеральным Законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» возможны следующие случаи взаимодействия Учреждения с субъектом ПДн, в которых необходимо обеспечить права и свободы гражданина:

получение ПДн с согласия субъекта ПДн (Приложения 5-6);

обработка обращений и запросов субъекта ПДн в Учреждении;

дополнительное взаимодействие с субъектом ПДн (в целях получения, уточнения ПДн, уведомления об изменениях, передача ПДн третьей стороне и т.д.) в процессе работы с ПДн ;

достижение цели обработки ПДн.

Ответственность за обеспечение безопасности ПДн при взаимодействии с субъектами ПДн и организацию работ по реагированию на обращения и запросы во всех перечисленных случаях несет руководитель структурного подразделения Учреждения, взаимодействующего с субъектами ПДн.

Работники данного структурного подразделения обязаны незамедлительно (в течение 1 рабочего дня) реагировать на обращения субъектов ПДн в следующих случаях:

обращение или запрос на получение информации, касающейся обработки ПДн субъекта ПДн;

требование уточнения ПДн;

отзыв согласия на обработку ПДн (Приложение 9).

XII. Обеспечение безопасности персональных данных при взаимодействии с контрагентами и третьими лицами

Учреждение в процессе осуществления своей деятельности может взаимодействовать с контрагентами и третьими лицами при обработке ПДн.

Взаимодействие с контрагентами и третьими лицами осуществляется в следующих случаях:

передача ПДн необходима в целях предупреждения угрозы жизни и здоровью субъекта ПДн или иных граждан;

передача ПДн в органы государственной власти или органы местного самоуправления на основании федеральных законов;

передача ПДн в органы государственной власти или органы местного самоуправления и негосударственные организации в целях оказания дополнительных услуг субъекту ПДн, предоставления субсидий и т.д.;

предоставление контрагенту доступа к ИСПДн в рамках исполнения договорных обязательств.

Передача ПДн контрагентам и третьим лицам, предоставление доступа к ПДн (за исключением случаев, установленных федеральными законами) регулируется договорными отношениями, предусматривающими обязательства третьей стороны по обеспечению информационной безопасности ПДн и заключение соглашения о конфиденциальности.

Работники Учреждения, осуществляющие обработку ПДн, должны руководствоваться следующими правилами передачи ПДн, предоставления доступа к ПДн:

ПДн запрещается передавать третьей стороне без письменного согласия субъекта ПДн (Приложение 8), за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также случаев, установленных федеральными законами;

передача ПДн третьей стороне допускается в минимальных объемах и только в целях выполнения задач, соответствующих причине передачи данных;

получение ПДн от третьих лиц допускается с согласия субъекта ПДн (Приложение 7);

предоставление третьей стороне (разработчикам, администраторам ИСПДн) доступа к ПДн допускается исключительно на основании письменного обращения, в объеме технологической необходимости, определяемой работниками отдела информационных технологий;

передача ПДн допускается при предупреждении лиц, получающих ПДн, о том, что эти данные могут быть использованы лишь в целях, в которых они переданы;

при передаче ПДн и предоставлении доступа к ПДн ведется учет лиц, которым переданы ПДн, предоставлен доступ к ПДн.

Решение о необходимости передачи ПДн и предоставлении доступа к ПДн принимается директором Учреждения.

XIII. Обязанности и ответственность работников Учреждения

Ответственность за организацию деятельности по обеспечению

информационной безопасности ПДн, обрабатываемых в Учреждении, возлагается на председателя Рабочей группы.

Ответственность за осуществление и контроль деятельности по обеспечению информационной безопасности ПДн, обрабатываемых в Учреждении, возлагается на работников отдела информационных технологий.

На руководителей структурных подразделений Учреждения, осуществляющих обработку ПДн, возлагаются следующие обязанности:

организация, учет и контроль доступа работников, допущенных к ПДн, в структурном подразделении;

уведомление работников, обрабатывающих ПДн, о факте обработки ими ПДн;

ознакомление работников, допущенных к обработке ПДн, с нормативными и организационно-распорядительными документами, обучение применению технических средств защиты информации;

контроль исполнения работниками должностных инструкций, в части обеспечения безопасности ПДн.

На работников отдела информационных технологий возлагаются следующие обязанности:

определение требований по информационной безопасности к СЗПДн Учреждения;

контроль реализации организационных и технических мер обеспечения информационной безопасности ПДн;

контроль выполнения работниками Учреждения, требований нормативных и организационно-распорядительных документов по обеспечению безопасности ПДн при их обработке;

организация эксплуатации программно-технических средств СЗПДн;

техническая реализация СЗПДн, ИСПДн.

На работников Учреждения, обрабатывающих ПДн, возлагаются обязанности по соблюдению требований нормативных и организационно-распорядительных документов Учреждения, регламентирующих получение, обработку и обеспечение безопасности ПДн.

Обязанности работников, возникающие в связи с защитой и обработкой ими ПДн, включаются в должностные инструкции работников.

Лица, виновные в нарушении требований по защите ПДн, несут ответственность в соответствии с законодательством Российской Федерации.

Приложение 1
к Положению

Форма

План мероприятий по защите персональных данных на____год (рекомендуемый)

Номер	Мероприятие	Срок выполнения	Ответственный	Примечание
1.				
2.				
3.				

Председатель рабочей группы _____ _____
(Подпись) (Инициалы, фамилия)
«_____»_____20___г.

Члены рабочей группы:

_____ _____ _____
(должность) (Подпись) (Инициалы, фамилия)
«_____»_____20___г.

_____ _____ _____

Приложение 2
к Положению

Форма

Перечень персональных данных,
обрабатывающихся в ГКУ «ЦБДДМО»

1 Наименование структурного подразделения:

Номер	Совокупность персональных данных	Основание для обработки	Цель и краткое описание порядка обработки	Срок и способ хранения, условия прекращения обработки
1.				
2.				
3.				

2 Наименование структурного подразделения:

Председатель рабочей группы _____ _____
(Подпись) (Инициалы, фамилия)

«____»_____20__г.

Члены рабочей группы:

_____ _____ _____
(должность) (Подпись) (Инициалы, фамилия)

Приложение 3
к Положению

Форма

Перечень информационных ресурсов,
содержащих персональные данные, в ГКУ «ЦБДДМО»

Номер	Совокупность информационных ресурсов, содержащие ПДн	Основание для обработки	Цель и краткое описание порядка обработки	Срок и способ хранения, условия прекращения обработки
1.				
2.				
3.				

Председатель рабочей группы _____ _____
(Подпись) (Инициалы, фамилия)

«____»_____20__г.

Члены рабочей группы:

_____ _____ _____
(должность) (Подпись) (Инициалы, фамилия)

Приложение 4
к Положению

Форма

Список работников, обрабатывающих персональные данные

Номер	Должность, подразделение работника	ПДн (согласно п.п. Перечня персональных данных), к обработке которых допущен работник	ИСПДн, в которой обрабатываются указанные сведения (при необходимости указывается конкретный модуль, информационный ресурс системы)
1.			
2.			
3.			

Приложение 5
к Положению

Форма

Согласие
на предоставление персональных данных и их обработку
(для работника)

1. Я,_____ (ФИО)
паспорт:_____, выдан:_____
_____,
дата выдачи: _____,
в соответствии с п. 4 ст. 9 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», свободно, по своей воле в государственное казенное учреждение Московской области «Центр безопасности дорожного движения Московской области» (далее - «Работодатель»), находящееся по адресу: 143441, Московская область, Красногорский район, п/о Путилково, 69 км МКАД, офисно-общественный комплекс ЗАО «Гринвуд», строение 7, на обработку свои персональные данные, необходимые для осуществления мной трудовых функций.

Перечень персональных данных, на обработку которых даю согласие: фамилия, имя, отчество, пол, дата и место рождения, гражданство, адрес регистрации и/или постоянного места жительства , номера служебных и личных телефонов, семейное положение, состав семьи, родственники, наличие иждивенцев, фотографии, образование,квалификация, наличие специальных знаний или специальной подготовки, трудовая деятельность до поступления на работу к Работодателю, занимаемые должности у Работодателя, содержание трудового договора, военно-учетные сведения, размер заработной платы, реквизиты банковской карты, сведения о постановке на учет в налоговых органах, о социальных льготах, о листах нетрудоспособности, о страховании, наличие судимостей, место работы или учебы членов семьи, родственников, иные сведения о работнике, необходимые в связи с трудовыми отношениями.

Предоставляю право осуществлять действия (операции) с персональными данными, включая заполнение и хранение документов, содержащих персональные данные работника: первичные документы по учету труда и его оплаты, утвержденные постановлением Госкомстата России №1 от 05.01.2004; приказы и указания Учреждения по личному составу и основной деятельности, содержащие персональные данные, материалы, сопровождающие оформление документов по учету труда и его оплаты

и содержащие основания к ним; личное дело и трудовая книжка работника; трудовые договоры; материалы по анкетированию, тестированию, проведению собеседований с кандидатами на должность, материалы, содержащие сведения об образовании, повышении квалификации и переподготовке, аттестации работника, доверенности на работника, отчетная, аналитическая и справочная информация, подготовленная с использованием персональных данных, отчеты, справки, направляемые в органы статистики, налоговые и правоохранительные органы, страховые агентства, военкоматы, органы специального страхования, пенсионные фонды, банки и другие организации, действующие в соответствии с законодательством, на основе персональных данных, иные документы, содержащие персональные данные.

С документами Работодателя, устанавливающими порядок обработки персональных данных, а также с моими правами и обязанностями в этой области ознакомлен.

2. Согласие предоставлено на срок, необходимый для осуществления целей обработки персональных данных, предусмотренных Федеральным законом. Согласие может быть отозвано мною в любое время на основании моего письменного заявления в соответствии с требованиями законодательства Российской Федерации.

«___»_____ ____ г.

Субъект персональных данных:

_____/_____
(подпись) (Ф.И.О.)

Приложение 6
к Положению

Форма

Согласие
на предоставление персональных данных и их обработку
(для иных субъектов персональных данных)

Я,_____ (ФИО)
паспорт:_____, выдан:_____
_____,
дата выдачи: _____,
в соответствии с п. 4 ст. 9 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», свободно, по своей воле даю согласие государственному казенному учреждению Московской области «Центр безопасности дорожного движения Московской области», находящемуся по адресу: 143441, Московская область, Красногорский район, п/о Путилково, 69 км МКАД, офисно-общественный комплекс ЗАО «Гринвуд», строение 7, на обработку моих персональных данных, а именно:
_____
_____,
то есть на совершение действий, предусмотренных п. 3 ст. 3 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

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

«___»_____ _____ г.

Субъект персональных данных:

_____/_____
(подпись) (Ф.И.О.)

Приложение 7
к Положению

Форма

Согласие
о получении персональных данных от третьих лиц

Я,_____ (ФИО)
паспорт:_____, выдан:_____
_____,
дата выдачи: _____,
не возражаю против получения Вами сведений обо мне, содержащих данные о
_____
(категории персональных данных)
в (из) _____,
(указать наименование юридического лица, откуда могут быть получены персональные данные)
в _____ форме в течение _____.
(документальной/электронной) (срок действия согласия)

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

«___»_____ _____ г.

Субъект персональных данных:

_____/_____
(подпись) (Ф.И.О.)

Приложение 8
к Положению

Форма

От _____

_____

(Ф.И.О.)

Зарегистрированный (ая) по адресу:

_____

Документ, удостоверяющий личность

_____

серия_____№_____

выдан_____

контактный телефон_____

Согласие
на передачу персональных данных третьей стороне

Я,_____ (ФИО)
даю согласие государственному казенному учреждения Московской области «Центр безопасности дорожного движения Московской области» свое согласие на предоставление _____
(указать наименование организации)
следующих моих персональных данных _____,
(перечислить персональные данные)
с целью _____

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

«___»_____ ____ г.

Субъект персональных данных:

_____/_____
(подпись) (Ф.И.О.)

Приложение 9
к Положению

Форма

От _____

_____

(Ф.И.О.)

Зарегистрированный (ая) по адресу:

_____

Документ, удостоверяющий личность

_____

серия_____№_____

выдан_____

контактный телефон_____

Отзыв согласия
на обработку персональных данных

Я,_____ (ФИО)
в соответствии с п. 2 ст. 9 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» отзываю у государственного казенного учреждения Московской области «Центр безопасности дорожного движения Московской области» свое согласие на обработку моих персональных данных.

Прошу прекратить обработку моих персональных данных в связи с _____,
в срок, не превышающий тридцати дней, с даты поступления настоящего отзыва.

«___»_____ ____ г.

Субъект персональных данных:

_____/_____
(подпись) (Ф.И.О.)