ПОЛОЖЕНИЕ
об обработке персональных данных в ГАУ «РМБИЦ»

1. Общие положения

1.1. Настоящее Положение разработано во исполнение Концепции информационной безопасности ГАУ «РМБИЦ» в соответствии с Трудовым кодексом Российской Федерации, Конституцией Российской Федерации, Гражданским кодексом Российской Федерации, Федеральным законом № 149-ФЗ от 26.07.2006 г. «Об информации, информационных технологиях и о защите информации», Федеральным законом «О персональных данных» от 27.07.06 № 152-ФЗ и другими нормативными правовыми актами и определяет порядок обработки персональных данных всех субъектов персональных данных, данные которых подлежат обработке в ГАУ «РМБИЦ» (далее Организация).
1.2. Требования настоящего Положения являются неотъемлемой частью комплекса мер безопасности и защиты информации в Организации.
1.3. Требования настоящего Положения распространяются на всех работников подразделений, осуществляющих обработку персональных данных в Организации.

2. Основные термины, сокращения и определения

2.1. Персональные данные — любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.
2.2. Обработка персональных данных — действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.
2.3. Конфиденциальность персональных данных — обязательное для соблюдения назначенного ответственного лица, получившего доступ к персональным данным, требование не допускать их распространения без согласия субъекта или иного законного основания.
2.4. Распространение персональных данных — действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.
2.5. Использование персональных данных — действия (операции) с персональными данными, совершаемые должностным лицом Организации в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении

субъектов либо иным образом затрагивающих их права и свободы или права и свободы других лиц.
2.6. Блокирование персональных данных — временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи.
2.7. Уничтожение персональных данных — действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.
2.8. Обезличивание персональных данных — действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту.
2.9. Общедоступные персональные данные — персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.
2.10. Информация — сведения (сообщения, данные) независимо от формы их представления.

3. Состав персональных данных

3.1. В состав персональных данных субъектов Организации входят:

3.1.1. Фамилия, имя, отчество.
3.1.2. Дата рождения
3.1.3. Место рождения
3.1.4. Адрес.
3.1.5. Семейное, социальное и имущественное положение.
3.1.6. Образование и специальность.
3.1.7. Профессия.
3.1.8. Должность.
3.1.9. Заработная плата (оклад, премии, надбавки).
3.1.10. Номера банковских расчетных счетов.
3.1.11. Сведения о социальных льготах.
3.1.12. Судимости и/или наличие обязательств по исполнительным листам.
3.1.13. Паспортные данные.
3.1.14. ИНН.
3.1.15. Информация о воинской обязанности.
3.1.16. Данные страхового полиса обязательного медицинского страхования.
3.1.17. Данные страхового полиса обязательного пенсионного страхования.
3.1.18. Трудовой и общий стаж.
3.1.19. Данные о предыдущих местах работы.
3.1.20. Фотография.
3.1.21. Адрес электронной почты.
3.1.22. Телефон (домашний, сотовый).
3.1.23. Фамилия, имя отчество, дата рождения детей.

3.2. В Организации создаются и хранятся следующие документы, содержащие данные о субъектах персональных данных:

3.2.1. Унифицированная форма Т-2 «Личная карточка работника».
3.2.2. Личное дело директора.
3.2.3. Приказы директора по личному составу.
3.2.4.Докладные записки, объяснительные записки нарушителей трудовой дисциплины.

3.2.5.Журнал учета личных дел.
3.2.6. Книга учета приказов по личному составу.
3.2.7. Трудовые книжки.
3.2.8. Заявления работника – субъекта персональных данных.
3.2.9. Договора на оказание услуг сторонними организациями.
3.2.10. Списки работников, подлежащих периодическому медицинскому осмотру.
3.2.11. Направления на обучение и курсы повышения квалификации.
3.2.12. Журнал регистрации вводного инструктажа.
3.2.13. Материалы расследований несчастных случаев на производстве.
3.2.14. Дипломы на специальности.
3.2.15. картотека читательских формуляров.
3.2.16. Командировочные удостоверения
3.2.17. Больничные листы.
3.2.18. Табеля учета рабочего времени.
3.2.19 Визитные карточки.
.

4. Цель обработки персональных данных

4.1. Целью обработки персональных данных субъектов является соблюдение трудового законодательства РФ, законодательства РФ об охране труда и техники безопасности, законодательства РФ об охране здоровья, заключение и исполнение договоров, стороной которых являются субъекты персональных данных, организация однократного пропуска субъекта персональных данных на территорию, на которой находится оператор, зачисление заработной платы работников на банковские карты, выпуск визитных карточек, размещение контактных данных руководителей на сайте Организации.
4.2. Условием прекращения обработки персональных данных является ликвидация Организации.

5. Сбор, обработка и защита персональных данных

5.1. Порядок получения (сбора) персональных данных:

5.1.1. Все персональные данные субъекта следует получать у него лично с его письменного согласия, кроме случаев, определенных в п. 5.1.4 и 5.1.6 настоящего Положения и иных случаях, предусмотренных законами.
5.1.2. Форма заявления-согласия субъекта, являющегося работником Организации, на обработку персональных данных представлена в приложении № 1 к настоящему положению. Форма заявления-согласия субъекта, не являющегося работником Организации, на обработку персональных данных представлена в приложении № 2 к настоящему положению.
5.1.3. Согласие субъекта на обработку персональных данных действует в течение неопределенного срока. Отзыв согласия на обработку персональных данных представлен в приложении № 3 к настоящему положению.
5.1.4. Если персональные данные субъекта возможно получить только у третьей стороны, субъект должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие (Приложение № 4 к настоящему положению). Третье лицо, предоставляющее персональные данные субъекта, должно обладать согласием субъекта на передачу персональных данных Организации. Организация обязана получить подтверждение от третьего лица, передающего персональные данные субъекта персональных данных о том, что персональные данные передаются с согласия субъекта. Организация обязана при взаимодействии с третьими лицами заключить с ними

соглашение о конфиденциальности информации, касающейся персональных данных субъектов.
5.1.5. Организация обязана сообщить субъекту персональных данных о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа субъекта персональных данных дать письменное согласие на их получение.
5.1.6. Обработка персональных данных субъектов без их согласия осуществляется в следующих случаях:
5.1.6.1. Персональные данные являются общедоступными.
5.1.6.2. По требованию полномочных государственных органов в случаях, предусмотренных федеральным законом.
5.1.6.3. Обработка персональных данных осуществляется на основании федерального закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия оператора.
5.1.6.4. Обработка персональных данных осуществляется в целях заключения и исполнения договора, одной из сторон которого является субъект персональных данных.
5.1.6.5. Обработка персональных данных осуществляется для статистических целей при условии обязательного обезличивания персональных данных.
5.1.6.6. В иных случаях, предусмотренных законом.
5.1.7. Организация не имеет права получать и обрабатывать персональные данные субъекта о его расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, интимной жизни.

5.2. Порядок обработки персональных данных:

5.2.1. Субъект персональных данных предоставляет сотруднику Организации, уполномоченному вести обработку персональных данных, достоверные сведения о себе.
5.2.2. На основании полученной информации сотрудник Организации проверяет наличие данного субъекта, зарегистрированного в информационной системе. Если субъект отсутствует в информационной системе, то операционный сотрудник заносит полную информацию о субъекте, после получения письменного согласия последнего. В случае наличия информации о субъекте в информационной системе – сверяет данные с ранее предоставленными (при необходимости вносит соответствующие изменения).
5.2.3. Своевременно, в срок не превышающий пяти рабочих дней, субъект персональных данных обязан лично или через своего законного представителя сообщать работнику, ответственному за сбор информации, об изменениях своих персональных данных с предоставлением соответствующих документов.
5.2.4. Организация обязуется прекратить обработку персональных данных в случае увольнения субъекта персональных данных.

5.3. Защита персональных данных:

5.3.1. Под защитой персональных данных субъекта понимается комплекс мер (организационно-распорядительных, технических, юридических), направленных на предотвращение неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных субъектов, а также от иных неправомерных действий.
5.3.2. Защита персональных данных субъекта осуществляется за счёт Организации в порядке, установленном соответствующими федеральными законами и внутренними организационными документами организации.

5.3.3. Организация при защите персональных данных субъектов принимает все необходимые организационно-распорядительные, юридические и технические меры, в том числе:
5.3.3.1. Шифровальные (криптографические) средства при передаче персональных данных.
5.3.3.2. Антивирусная защита.
5.3.3.3. Организация режима обеспечения безопасности помещений, в которых размещена информационная система и обрабатываются персональные данные, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения, а именно:

- Запрещение нахождение сотрудников в таких помещениях, в целях, не связанных со служебной деятельностью;
- Нахождение лиц, не участвующих в обработке персональных данных в таких помещениях возможно только в присутствии лиц, осуществляющих обработку персональных данных;
- После исполнения своих обязанностей в таких помещениях сотруднику необходимо убрать все документы ограниченного пользования в специально отведенное для этого место, выключить всю аппаратуру, если это не препятствует технологическому процессу обработки информации, запереть помещение.
- При начале работы, а также после продолжительного отсутствия на рабочем месте следует проверить отсутствие несанкционированного доступа в такое помещение, а при его обнаружении немедленно сообщить об этом факте начальнику службы охраны и заведующему WEB-узла.

Перечень помещений, в которых обрабатываются персональные данные субъектов, приведен в Приложении № 5 к настоящему положению.
5.3.3.4. Обеспечение сохранности и учета носителей персональных данных.
5.3.3.5. Утверждение руководителем оператора перечня лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных обязанностей.
5.3.3.6. Назначение приказом руководителя Организации должностного лица, ответственного за обеспечение безопасности персональных данных в информационной системе и утверждение должностного регламента такого лица (Приложение №6).
5.3.3.7. Создание резервных копий персональных данных.
5.3.3.8. Издание нормативно-методических локальных актов, регулирующих защиту персональных данных.

6. Блокировка, обезличивание, уничтожение персональных данных

6.1. Порядок блокировки и разблокировки персональных данных:

6.1.1. Блокировка персональных данных субъектов осуществляется с письменного заявления субъекта персональных данных.
6.1.2. Блокировка персональных данных подразумевает:
6.1.2.1. Запрет редактирования персональных данных.
6.1.2.2. Запрет распространения персональных данных любыми средствами (e-mail, сотовая связь, материальные носители).
6.1.2.3. Запрет использования персональных данных в массовых рассылках (sms, e-mail, почта).
6.1.2.4. Запрет открытия банковских счетов.
6.1.2.5. Изъятие бумажных документов, относящихся к субъекту персональных данных и содержащих его персональные данные из внутреннего документооборота Организации и запрет их использования.

6.1.3. Блокировка персональных данных субъекта может быть временно снята, если это требуется для соблюдения законодательства.
6.1.4. Разблокировка персональных данных субъекта осуществляется с его письменного согласия или заявления.
6.1.5. Повторное согласие субъекта персональных данных на обработку его данных влечет разблокирование его персональных данных.

6.2. Порядок обезличивания и уничтожения персональных данных:

6.2.1. Обезличивание персональных данных субъекта происходит по письменному заявлению субъекта персональных данных, при условии, что все договорные отношения завершены и от даты окончания последнего договора прошло не менее 5 лет.
6.2.2. При обезличивании персональные данные в информационных системах заменяются набором символов, по которому невозможно определить принадлежность персональных данных к конкретному субъекту.
6.2.3. Бумажные носители документов при обезличивании персональных данных уничтожаются. В случае невозможности уничтожения бумажных носителей, содержащих персональные данные как обезличиваемого субъекта, так и других субъектов персональных данных, персональные данные уничтожаются путем стирания или замазывания.
6.2.4. Операция обезличивания персональных данных субъекта необратима.
6.2.5. Организация обязана обеспечить конфиденциальность в отношении персональных данных при необходимости проведения испытаний информационных систем на территории разработчика и произвести обезличивание персональных данных в передаваемых разработчику информационных системах.
6.2.6. Уничтожение персональных данных субъекта подразумевает прекращение какого-либо доступа к персональным данным субъекта.
6.2.7. При уничтожении персональных данных субъекта работники Организации не могут получить доступ к персональным данным субъекта в информационных системах.
6.2.8. Бумажные носители документов при уничтожении персональных данных уничтожаются, персональные данные в информационных системах обезличиваются. Персональные данные восстановлению не подлежат.
6.2.9. Операция уничтожения персональных данных необратима.

7. Передача и хранение персональных данных

7.1. Передача персональных данных:

7.1.1. Под передачей персональных данных субъекта понимается распространение информации по каналам связи и на материальных носителях.
7.1.2. При передаче персональных данных работники Организации должны соблюдать следующие требования:
7.1.2.1. Не сообщать персональные данные субъекта в коммерческих целях. Обработка персональных данных субъектов в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи не допускается.
7.1.2.2. Осуществлять передачу персональных данных субъектов в пределах Организации в соответствии с настоящим Положением, нормативно-технологической документацией и должностными инструкциями.
7.1.2.3. Разрешать доступ к персональным данным только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы для выполнения должностных обязанностей.

7.1.2.4. Передавать персональные данные субъекта представителям субъекта в порядке, установленном законодательством и нормативно-технологической документацией и ограничивать эту информацию только теми персональными данными субъекта, которые необходимы для выполнения указанными представителями их функции.

7.2. Хранение и использование персональных данных:

7.2.1. Под хранением персональных данных понимается существование записей в информационных системах и на материальных носителях.
7.2.2. Персональные данные субъектов обрабатываются и хранятся в информационных системах, а также на бумажных носителях в Организации.
7.2.3. Хранение персональных данных субъектов осуществляется кадровой службой, бухгалтерией, сметно-договорным отделом, отделом по охране труда и технике безопасности, профкомом, службой охраны на бумажных и электронных носителях с ограниченным доступом.
7.2.4 Личные дела хранятся в бумажном виде в папках, прошитые и пронумерованные по страницам. Личные дела хранятся в специально отведенной секции сейфа, обеспечивающего защиту от несанкционированного доступа.
7.2.5. Подразделения, хранящие персональные данные на бумажных носителях, обеспечивают их защиту от несанкционированного доступа и копирования согласно «Положению об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утвержденному постановлением правительства РФ 15 сентября 2008 г. N 687.
7.2.6. Срок хранения персональных данных субъекта определяется на основе соответствующих федеральных законов и внутренних нормативных документов Организации.

8. Доступ к персональным данным

8.1. Право доступа к персональным данным субъектов имеют работники Организации, входящие в перечень лиц, осуществляющих обработку персональных данных (Приложение №7). Должностное лицо Организации, имеющее доступ к обработке персональных данных фиксируется в журнале о допуске к персональным данным (Приложение №8).
8.2. Работники Организации, получившие доступ к персональным данным субъекта, обязаны использовать их лишь в целях, для которых сообщены персональные данные и обязаны соблюдать режим секретности (конфиденциальности) обработки и использования полученной информации (персональных данных субъектов).
8.3. К числу массовых потребителей персональных данных вне учреждения относятся государственные и негосударственные функциональные структуры: налоговые инспекции; правоохранительные органы; органы статистики; страховые агентства; военкоматы; органы социального страхования; пенсионные фонды; подразделения федеральных, республиканских и муниципальных органов управления. Надзорно-контрольные органы имеют доступ к информации только в сфере своей компетенции.
8.4. Организации, в которые субъект может осуществлять перечисления денежных средств (страховые Общества, негосударственные пенсионные фонды, благотворительные организации, кредитные учреждения) могут получить доступ к персональным данным субъекта только в случае его письменного разрешения.
8.3. Субъект может получить доступ к своим персональным данным на основании письменного запроса или при обращении, включая право на безвозмездное получение копий любой записи, содержащей персональные данные субъекта.

8.4. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных оператором, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.
8.5. Обращение субъекта или поступивший запрос рассматривается должностным лицом Организации, ответственным за обеспечение безопасности персональных данных в информационной системе.
8.6. В случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта персональных данных или его представителя ответственный за обеспечение безопасности персональных данных в информационной системе готовит в письменной форме мотивированный ответ, содержащий ссылку на положение федерального закона, являющееся основанием для такого отказа, в срок, не превышающий тридцати дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя.
8.7. Организация предоставляет безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных.
8.8. В срок, не более семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, Организация вносит в них необходимые изменения.
С этой целью ответственный за обеспечение безопасности персональных данных дает поручение должностному лицу Организации, входящему в Перечень лиц, осуществляющих обработку персональных данных, внести изменения в персональные данные субъекта.
8.9. В срок, не более семи рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, Организация уничтожает такие персональные данные и уведомляет субъекта персональных данных или его представителя о внесенных изменениях и предпринятых .
8.10. Организация сообщает в уполномоченный орган по защите прав субъектов персональных данных по запросу этого органа необходимую информацию в течение тридцати дней с даты получения такого запроса.

9. Права оператора персональных данных

Организация вправе:
9.1. Отстаивать свои интересы в суде.
9.2. Предоставлять персональные данные субъектов третьим лицам, если это предусмотрено действующим законодательством (налоговые, правоохранительные органы и др.).
9.3. Отказать в предоставлении персональных данных в случаях предусмотренных законом.

9.4. Использовать персональные данные субъекта без его согласия, в случаях предусмотренных законом.
9.5. Осуществлять внутренний контроль за соблюдением настоящего Положения согласно должностному регламенту специалиста по обеспечению безопасности персональных данных.
9.6. Проводить расследование инцидентов безопасности персональных данных на основании принятого в организации Регламента реагирования на инциденты информационной безопасности.

10. Права субъекта персональных данных

Субъект персональных данных имеет право:
10.1. Требовать уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав;
10.2. Требовать перечень обрабатываемых персональных данных, имеющихся в Организации и источник их получения.
10.3. Получать информацию о сроках обработки персональных данных, в том числе о сроках их хранения.
10.4. Требовать извещения всех лиц, которым ранее были сообщены неверные или неполные его персональные данные, обо всех произведенных в них исключениях, исправлениях или дополнениях.
10.5. Обжаловать в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке неправомерные действия или бездействия при обработке его персональных данных.

11. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных

11.1. Работники Организации, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.
11.2. Работники организации, осуществляющие обработку персональных данных, обязаны подписать соглашение о неразглашении персональных данных. Форма соглашения о неразглашении персональных данных представлена в приложении №9 настоящего положения.