

ПОЛИТИКА

ГБУЗ НО «НОЦК» в отношении обработки персональных данных и сведения о реализуемых требованиях к защите персональных данных

1. Общие положения

1.1. Политика ГБУЗ НО «НОЦК» в отношении обработки персональных данных и сведения о реализуемых требованиях к защите персональных данных (далее - Политика) определяет общие принципы и порядок обработки персональных данных, меры по обеспечению их безопасности в ГБУЗ НО «НОЦК» (далее - Оператор).

Целью Политики является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну, четкое и неукоснительное соблюдение требований российского законодательства в области персональных данных.

1.2. Политика разработана в соответствии с положениями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», другими законодательными и нормативными правовыми актами, определяющими порядок работы с персональными данными и требования к обеспечению их безопасности.

1.3. В Политике используются следующие термины и определения:

Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники.

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.

Блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Доступ к персональным данным - ознакомление определенных лиц (в том числе работников) с персональными данными субъектов, обрабатываемыми Оператором, при условии сохранения конфиденциальности этих сведений.

Интернет-сайт (Сайт) - совокупность программ для электронных вычислительных машин и иной информации, содержащейся в информационной системе, доступ к которой обеспечивается посредством информационно-телекоммуникационной сети интернет по доменным именам и (или) по сетевым адресам, позволяющим идентифицировать сайты в сети интернет. В Политике под Сайтом понимается сайт Оператора ГБУЗ НО «НОЦК».

Конфиденциальность персональных данных - обязанность лиц, получивших доступ к персональным данным, не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено законодательством.

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.

Общедоступные персональные данные - персональные данные, доступ неограниченного круга лиц к которым предоставлен на основании законодательства,

субъектом персональных данных либо по его просьбе, в том числе данные, которые подлежат обязательному раскрытию или опубликованию.

Оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующее и (или) осуществляющее обработку персональных данных, а также определяющее цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными. В Политике под оператором понимается ГБУЗ НО «НОЦК».

Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Страница сайта в сети интернет (Интернет-страница) - часть сайта в сети интернет, доступ к которой осуществляется по указателю, состоящему из доменного имени и символов, определенных владельцем сайта в сети интернет. В Политике под Интернет-страницами понимаются страницы Сайта ГБУЗ НО «НОЦК»

Субъект персональных данных - физическое лицо, к которому относятся персональные данные.

Субъект обращения донорской крови и ее компонентов - организации, осуществляющие деятельность в сфере обращения донорской крови и ее компонентов

Трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

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.

2. Статус Оператора и категории субъектов, чьи персональные данные обрабатываются Оператором

2.1. Оператор является оператором персональных данных в отношении персональных данных следующих физических лиц:

- работников Оператора, с которыми заключены трудовые договоры, а также лиц, выполняющих работы в интересах Оператора в соответствии с заключенными с ними гражданско-правовыми договорами (далее - **Работники**);
- близких родственников работников Оператора, обработка персональных данных которых предусмотрена законодательством, а также выполняется Оператором как работодателем в соответствии с требованиями органов государственного статистического учета (далее - **Родственники работников**);
- соискателей вакантных должностей Оператора, представивших лично или через специализированные организации по подбору персонала (кадровые агентства) свои резюме или анкеты (далее - **Соискатели**);
- субъектов персональных данных, (далее - **Субъекты**);
- представителей субъектов персональных данных, обращающихся к Оператору по поручению и от имени субъектов персональных данных (далее - **Представители субъектов**);
- посетителей территорий и помещений Оператора, которым необходимо оформление разового пропуска (далее - **Посетители**).

2.2. Оператор является лицом, организующим обработку персональных данных по поручению других операторов, к которым относятся (не исчерпывая):

- органы власти, финансовые организации и государственные внебюджетные фонды, в которые перечисляются средства Работников или средства для зачисления на счет Работников (инспекции Федеральной налоговой службы, территориальные отделения Пенсионного фонда Российской Федерации, Федерального фонда обязательного медицинского страхования, Фонда социального страхования Российской Федерации др.);
- военные комиссариаты, профсоюзные органы, которым персональные данные предоставляются (передаются) в случаях, предусмотренных законодательством;
- субъекты обращения донорской крови и ее компонентов.

Указанным выше операторам персональные данные предоставляются (передаются) в объеме, определенном законодательством, соответствующими органами власти и государственными внебюджетными фондами в пределах их полномочий. Специального согласия субъектов на такую передачу персональных данных не требуется.

3. Принципы обработки персональных данных

Обработка персональных данных Оператором осуществляется в соответствии со следующими принципами:

3.1. Законность и справедливая основа обработки персональных данных. Оператор принимает все необходимые меры по выполнению требований законодательства, не обрабатывает персональные данные в случаях, когда это не допускается законодательством, не использует персональные данные во вред субъектам.

3.2. Ограничение обработки персональных данных достижением конкретных, заранее определённых и законных целей. Целями обработки персональных данных Оператором являются:

- в отношении Работников - соблюдение законов и иных нормативных правовых актов, содействие работникам в трудоустройстве, получении образования и продвижении по службе, обеспечение личной безопасности работников, контроль количества и качества выполняемой работы и обеспечения сохранности имущества, расчет и выплата заработной платы, иных вознаграждений, расчет и перечисление налогов и страховых взносов;
- в отношении Родственников работников - предоставление Работникам льгот и гарантий, предусмотренных законодательством для лиц, имеющих (усыновивших) детей, лиц с семейными обязанностями, выполнение требований нормативных правовых актов органов государственного статистического учета;
- в отношении Соискателей - принятие решения о возможности замещения вакантных должностей кандидатами, наиболее полно соответствующими требованиям Оператора;
- в отношении Субъектов – обеспечение безопасности донорской крови и ее компонентов и сохранение здоровья доноров при выполнении ими донорской функции;
- в отношении Представителей субъектов - выполнение Оператором действий по поручению представителей субъектов персональных данных;
- в отношении Посетителей - обеспечение возможности прохода в помещения Оператора лиц, не имеющих постоянных пропусков.

3.3. Обработка только тех персональных данных, которые отвечают заранее объявленным целям их обработки. Соответствие содержания и объёма

обрабатываемых персональных данных заявленным целям обработки. Недопущение обработки персональных данных, не совместимой с целями сбора персональных данных, а также избыточных по отношению к заявленным целям их обработки. Оператор заявляет, что не собирает и не обрабатывает персональные данные, не требующиеся для достижения целей, указанных в п.3.2 Политики, не использует персональные данные субъектов в каких-либо целях, отличных от указанных выше.

3.4. Недопущение объединения баз данных, содержащих персональные данные, обработка которых осуществляется в целях, не совместимых между собой.

3.5. Обеспечение точности, достаточности и актуальности персональных данных по отношению к целям обработки персональных данных. Оператор принимает все разумные меры по поддержке актуальности обрабатываемых персональных данных, включая, но не ограничиваясь, реализацией права каждого субъекта получать для ознакомления свои персональные данные и требовать от Оператора их уточнения, блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленных выше целей обработки.

3.6. Хранение персональных в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен законодательством, договором, стороной которого является субъект персональных данных.

3.7. Уничтожение либо обезличивание персональных данных по достижении заявленных целей их обработки или в случае утраты необходимости в достижении этих целей, при невозможности устранения Оператором допущенных нарушений установленного законодательством порядка обработки персональных данных, отзыве согласия на обработку субъектом персональных данных, если иное не предусмотрено законодательством или договорами с субъектами.

4. Условия обработки персональных данных

4.1. Обработка персональных данных Оператором допускается в следующих случаях:

4.1.1. При наличии письменного согласия субъекта персональных данных на обработку его персональных данных. Порядок получения Оператором согласия субъекта персональных данных определен в разделе 7 Политики.

4.1.2. Обработка персональных данных необходима для осуществления и выполнения возложенных законодательством на Оператора функций, полномочий и обязанностей. К таким случаям, в том числе, относится, не исчерпывая их, обработка специальных категорий персональных данных Работников для достижения целей, предусмотренных трудовым и пенсионным законодательством.

4.1.3. Для исполнения договора, стороной которого является субъект персональных данных, для заключения договора по инициативе субъекта персональных данных, а также для исполнения договора между Оператором и образовательной организацией, преподавателем (представителем администрации), стороной которого является субъект персональных данных. Такими договорами являются:

- трудовые, гражданско-правовые договоры с Работниками Оператора.

Преддоговорной работой является работа по подбору персонала, в которой согласие субъекта на обработку подтверждается собственноручно заполненной анкетой Соискателя или анкетой (резюме), переданной им Оператору, в специализированную организацию по подбору персонала, размещенной Соискателем на специализированных сайтах в сети интернет или присланной Соискателем Оператору по электронной почте.

4.1.4. 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 субъектов персональных данных.

4.1.5. Обработка персональных данных осуществляется в статистических или иных исследовательских целях при условии обязательного обезличивания персональных данных.

4.1.6. Доступ неограниченного круга лиц к персональным данным предоставлен субъектом персональных данных лично, либо по его просьбе.

4.1.7. Персональные данные подлежат опубликованию или обязательному раскрытию в соответствии с действующим законодательством

4.2. Оператор не раскрывает третьим лицам и не распространяет персональные данные без согласия субъекта персональных данных, если иное не предусмотрено законодательством или договором с субъектом персональных данных.

4.3. Оператор обрабатывает персональные данные, относящиеся к специальным категориям и касающиеся состояния здоровья, а в отношении Работников - только сведения, относящиеся к вопросу о возможности выполнения Работником трудовой функции

4.4. Обработка персональных данных о судимости может осуществляться Оператором исключительно в случаях и в порядке, установленных законодательством.

4.5. Оператор обрабатывает биометрические персональные данные доноров по их письменному согласию.

4.6. Оператор не осуществляет трансграничную передачу персональных данных.

4.7. Оператор не принимает решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих права и законные интересы субъекта, на основании исключительно автоматизированной обработки персональных данных. Данные, имеющие юридические последствия или затрагивающие права и законные интересы субъекта, подлежат перед их использованием проверке уполномоченными работниками Оператора.

5. Способы обработки персональных данных

5.1. Оператор осуществляет обработку персональных данных с использованием средств автоматизации, а также без использования таких средств.

5.2. Политика распространяется в полном объеме на обработку персональных данных с использованием средств автоматизации, а при обработке без использования средств автоматизации - только на случаи, если обработка соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации, то есть позволяет осуществлять в соответствии с заданным алгоритмом поиск персональных данных, зафиксированных на материальном носителе и содержащихся в картотеках или иных систематизированных собраниях персональных данных, и (или) осуществлять доступ к таким персональным данным.

6. Конфиденциальность персональных данных

6.1. Работниками Оператора, получившими доступ к персональным данным, обеспечивается конфиденциальность таких данных.

Обеспечение конфиденциальности не требуется в отношении:

- персональных данных после их обезличивания;
- общедоступных персональных данных.

6.2. Оператор вправе с согласия субъекта поручить обработку персональных данных другому лицу, если иное не предусмотрено законодательством, на основании заключаемого с этим лицом договора, предусматривающего в качестве существенного условия обязанность лица, осуществляющего обработку персональных данных по

поручению Оператора, соблюдать принципы и правила обработки персональных данных, предусмотренные законодательством. Объем передаваемых другому лицу для обработки персональных данных и количество используемых этим лицом способов обработки должны быть минимально необходимыми для выполнения им своих обязанностей перед Оператором. В поручении Оператора должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со статьей 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

- 6.3. Данные о донорах и лицах отведенных от донорства, содержатся в региональном сегменте ЕИБД.
- 6.4. В случае, если Оператор поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет Оператор. Лицо, осуществляющее обработку персональных данных по поручению Оператора, несет ответственность перед Оператором.

7. Согласие субъекта персональных данных на обработку своих персональных данных

7.1. Субъект персональных данных принимает решение о предоставлении его персональных данных Оператору и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку персональных данных должно быть конкретным, информированным и сознательным и может предоставляться субъектом в любой позволяющей подтвердить факт его получения форме, если иное не установлено законодательством.

7.2. В случае получения согласия на обработку персональных данных от Представителя субъекта персональных данных полномочия данного представителя на дачу согласия от имени субъекта персональных данных проверяются Оператором.

7.3. В случае получения Оператором персональных данных от различных медицинских организаций (Постановление правительства 667 от 5.08.13) ответственность за правомерность и достоверность персональных данных, а также за получение согласия субъектов (их представителей) на передачу их персональных данных Оператору несет образовательная организация, передающее персональные данные.

7.4. Оператор, получивший персональные данные, не принимает на себя обязательства по информированию субъектов (их представителей), чьи персональные данные ей переданы, о начале обработки персональных данных, полагая, что они проинформированы об этом передавшей персональные данные организациями при получении согласия на такую передачу.

7.5. Специального выраженного согласия Работника на обработку его персональных данных не требуется, так как обработка необходима для исполнения трудового договора, стороной которого является Работник-субъект персональных данных, за исключением случаев, когда необходимо получение согласия Работника в письменной форме для конкретных случаев обработки персональных данных.

7.6. Специального выраженного согласия Родственников работников Оператора не требуется, если обработка их персональных данных осуществляется на основании законодательства (для получения алиментов, оформления социальных выплат и пр.), а также выполняется Оператором как работодателем в соответствии с требованиями органов государственного статистического учета. Во всех остальных случаях необходимо получение доказываемого (подтверждаемого) согласия Родственников работников на обработку их персональных данных Оператором.

7.7. Специального выраженного согласия Соискателя на обработку его персональных данных не требуется, так как обработка необходима в целях заключения трудового договора по инициативе Соискателя-субъекта персональных данных, за исключением случаев, когда необходимо получение согласия Соискателя в письменной форме для конкретных случаев обработки персональных данных. В случае принятия решения об отказе Соискателю в приеме на работу его персональные данные должны быть уничтожены в течение 30 дней с даты принятия такого решения.

7.8. Не требуется специального выраженного согласия Субъектов и их Представителей на обработку персональных данных, которые в соответствии с законодательством о СМИ являются открытыми и общедоступными.

7.9. Согласие Посетителя на обработку персональных данных дается в форме конклюдентных действий, выражающихся либо в предоставлении своих персональных данных, необходимых для входа в офис Оператора, либо в форме передачи документа, удостоверяющего личность, работникам службы охраны.

7.10. Согласие субъектов на предоставление их персональных данных не требуется при получении Оператором, в рамках установленных полномочий, мотивированных запросов от органов прокуратуры, правоохранительных органов, органов безопасности, от государственных инспекторов труда при осуществлении ими государственного надзора и контроля за соблюдением трудового законодательства и иных органов, уполномоченных запрашивать информацию в соответствии с компетенцией, предусмотренной законодательством.

Мотивированный запрос должен включать в себя указание цели запроса, ссылку на правовые основания запроса, в том числе подтверждающие полномочия органа, направившего запрос, а также перечень запрашиваемой информации.

7.11. В случае поступления запросов из организаций, не обладающих соответствующими полномочиями, Оператор обязан получить согласие субъекта на предоставление его персональных данных и предупредить лиц, получающих персональные данные, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, а также требовать от этих лиц подтверждения того, что это правило будет (было) соблюдено.

7.12. Согласие на обработку персональных данных, обработка которых не установлена требованиями законодательства или не требуется для исполнения договора с Оператором, стороной которого является субъект персональных данных, может быть отозвано субъектом персональных данных.

Оператор вправе продолжить обработку персональных данных и после отзыва согласия субъекта, если эти данные в соответствии с законодательством являются открытыми и общедоступными, однако доступ к ним лиц, не являющихся работниками Оператора, прекращается.

7.13. Во всех случаях обязанность предоставить доказательство получения согласия субъекта персональных данных на обработку его персональных данных или доказательство наличия оснований, указанных в Федеральном законе от 27.07.2006 № 152-ФЗ «О персональных данных», возлагается на Оператора.

8. Права субъектов персональных данных

8.1. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных и установленной законодательством.

8.2. Субъект персональных данных вправе требовать от Оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законодательством меры по защите своих прав.

8.3. Если субъект персональных данных считает, что Оператор осуществляет обработку его персональных данных с нарушением требований федеральных законов или иным

образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие Оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

8.4. Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

9. Сведения о реализуемых требованиях к защите персональных данных

9.1. Защита персональных данных, обрабатываемых Оператором, обеспечивается реализацией правовых, организационных и технических мер, необходимых и достаточных для обеспечения требований законодательства в области защиты персональных данных.

9.2. Правовые меры включают:

- разработку локальных актов Оператора, реализующих требования законодательства, в том числе - Положения о порядке обработки и обеспечении безопасности персональных данных и Политики, размещение Политики на Сайте Оператора;
- отказ от любых способов обработки персональных данных, не соответствующих определенным в Политике целям.

9.3. Организационные меры включают:

- назначение лица, ответственного за организацию обработки персональных данных;
- назначение лица, ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных;
- ограничение состава работников Оператора, имеющих доступ к персональным данным, и организацию разрешительной системы доступа к ним;
- ознакомление работников Оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства о персональных данных, в том числе с требованиями к защите персональных данных, с Положением об обработке персональных данных, другими локальными актами Оператора по вопросам обработки персональных данных;
- обучение всех категорий работников, непосредственно осуществляющих обработку персональных данных, правилам работы с ними и обеспечения безопасности обрабатываемых данных;
- определение в должностных инструкциях работников Оператора обязанностей по обеспечению безопасности обработки персональных данных и ответственности за нарушение установленного порядка;
- регламентацию процессов обработки персональных данных;
- организацию учёта материальных носителей персональных данных и их хранения, обеспечивающих предотвращение хищения, подмены, несанкционированного копирования и уничтожения;
- определение угроз безопасности персональных данных при их обработке в информационных системах, формирование на их основе модели (моделей) угроз;
- размещение технических средств обработки персональных данных в пределах охраняемой территории;
- ограничение допуска посторонних лиц в помещения Оператора, недопущение их нахождения в помещениях, где ведется работа с персональными данными и размещаются технические средства их обработки, без контроля со стороны работников Оператора.

9.4. Технические меры включают:

- определение типа угроз безопасности персональных данных, актуальных для информационных систем персональных данных с учетом оценки возможного вреда субъектам персональных данных, который может быть причинен в случае нарушения требований безопасности, определение уровня защищенности персональных данных и реализацию требований к защите персональных данных при их обработке в

информационных системах, исполнение которых обеспечивает установленные уровни защищенности персональных данных;

- разработку на основе модели угроз системы защиты персональных данных для установленных Правительством Российской Федерации уровней защищенности персональных данных при их обработке в информационных системах;
- использование для нейтрализации актуальных угроз средств защиты информации, прошедших процедуру оценки соответствия;
- оценку эффективности принимаемых мер по обеспечению безопасности персональных данных;
- реализацию разрешительной системы доступа работников к персональным данным, обрабатываемым в информационных системах, и программно-аппаратным и программным средствам защиты информации;
- регистрацию и учёт действий с персональными данными пользователей информационных систем, где обрабатываются персональные данные;
- выявление вредоносного программного обеспечения (применение антивирусных программ) на всех узлах информационной сети Оператора, обеспечивающих соответствующую техническую возможность;
- безопасное межсетевое взаимодействие (применение межсетевого экранирования);
- обнаружение вторжений в информационную систему Оператора, нарушающих или создающих предпосылки к нарушению установленных требований по обеспечению безопасности персональных данных;
- восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним (систему резервного копирования и восстановления персональных данных);
- периодическое проведение мониторинга действий пользователей, разбирательств по фактам нарушения требований безопасности персональных данных;
- контроль за выполнением настоящих требований (самостоятельно или с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации) не реже 1 раза в 3 года.

10. Заключительные положения

10.1. Иные обязанности и права Оператора как оператора персональных данных и лица, организующего их обработку по поручению других операторов, определяются законодательством Российской Федерации в области персональных данных.

10.2. Должностные лица и работники Оператора, виновные в нарушении норм, регулирующих обработку и защиту персональных данных, несут материальную, дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством.

10.3. Положения Политики пересматриваются по мере необходимости. Обязательный пересмотр Политики проводится в случае существенных изменений международного или национального законодательства в сфере персональных данных.

При внесении изменений в положения Политики учитываются:

- изменения в информационной инфраструктуре и (или) в используемых Оператором информационных технологиях;
- сложившаяся в Российской Федерации практика правоприменения законодательства в области персональных данных;
- изменение условий и особенностей обработки персональных данных Оператором в связи с внедрением в его деятельность новых информационных систем, процессов и технологий.