

ПОЛИТИКА

**Общества с ограниченной ответственностью «Рош Диабетес Кеа Рус»
в отношении обработки персональных данных и сведения о реализуемых
требованиях к защите персональных данных**

Москва, 2024

1. Общие положения

1.1. «Политика Общества с ограниченной ответственностью «Рош Диабетес Кеа Рус» в отношении обработки персональных данных и сведения о реализуемых требованиях к защите персональных данных» (далее – Политика) определяет общие принципы и порядок обработки персональных данных и меры по обеспечению их безопасности в ООО «Рош- Диабетес Кеа Рус» (далее – Общество).

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 Российской Федерации в области персональных данных (далее – законодательство).

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;

база персональных данных – упорядоченный массив персональных данных, независимый от вида материального носителя информации и используемых средств его обработки (архивы, картотеки, электронные базы данных);

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, когда обработка необходима для уточнения персональных данных);

веб-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 веб-сайты в сети «Интернет»;

дата-центр – специализированная организация, предоставляющая услуги по размещению серверного и сетевого оборудования, сдаче серверов (в том числе виртуальных) в аренду, а также по подключению к сети «Интернет»;

доступ к персональным данным – ознакомление определенных лиц (в том числе работников) с персональными данными субъектов, обрабатываемыми Обществом, при условии сохранения конфиденциальности этих сведений;

информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

использование персональных данных – действия (операции) с персональными данными, совершаемые оператором в целях принятия решений и/или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц, либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц;

контрагент – сторона договора с Обществом, не являющаяся работником Общества;

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;

облачная вычислительная инфраструктура – общий пул конфигурируемых вычислительных ресурсов (сети передачи данных, серверы, устройства хранения данных, приложения и сервисы – как вместе, так и по отдельности), к которым обеспечен повсеместный и удобный сетевой доступ по требованию, и которые могут быть оперативно предоставлены и освобождены с минимальными эксплуатационными затратами или обращениями к провайдеру, обладающие пятью основными свойствами: самообслуживание по требованию, универсальный доступ по сети, объединение ресурсов, эластичность, учёт потребления;

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 с согласия субъекта персональных данных либо по его просьбе, а также данные, которые подлежат обязательному раскрытию или опубликованию в соответствии с требованиями законодательства;

Общество – Общество с ограниченной ответственностью «Рош Диабетес Кеа Рус»;

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 Общество, если иное не указано специально;

персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

персональные данные, разрешенные субъектом персональных данных для распространения – персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном Федеральным законом «О 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;

Роскомнадзор – Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций, на которую возложены функции уполномоченного органа по защите прав субъектов персональных данных, а также функции по федеральному государственному контролю (надзору) за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных;

сведения о состоянии здоровья – сведения о результатах медицинского обследования, наличии заболевания, об установленном диагнозе и о прогнозе развития заболевания, методах оказания медицинской помощи, связанном с ними риске, возможных видах медицинского вмешательства, его последствиях и результатах оказания медицинской помощи;

специальные категории персональных данных – сведения, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни;

страница веб-сайта – часть веб-сайта, доступ к которой осуществляется по указателю, состоящему из доменного имени и символов, определенных владельцем веб-сайта;

субъект персональных данных – физическое лицо, к которому относятся персональные данные;

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 Общества и категории субъектов, чьи персональные данные обрабатываются Обществом

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

- работников Общества, с которыми заключены или были заключены трудовые договоры, в том числе те, с которыми трудовые договоры уже прекращены (расторгнуты) (далее – **Работники**);
- работников иных компаний группы Roche (далее – **Работники компаний группы**);
- близких родственников, супругов и лиц, находящихся на иждивении Работников, в том числе бывших супругов, которым выплачиваются алименты (далее – **Члены семей работников**);
- физических лиц – представителей органов управления и учредителей участников Общества, не являющиеся его работниками (далее – **Руководители и учредители**);
- соискателей вакантных должностей Общества (кандидатов для приема на работу Обществом), представивших свои резюме или анкеты, содержащие персональные данные, лично или через специализированные организации по подбору персонала (кадровые агентства), в том числе через специализированные веб-сайты в сети Интернет, а также в отношении которых Обществом проявлена инициатива о найме на работу (далее – **Соискатели**);

*Политика в отношении обработки персональных данных
и сведения о реализуемых требованиях к защите персональных данных*

- представителей контрагентов-юридических лиц и индивидуальных предпринимателей, в том числе работников, владельцев, включая бенефициарных владельцев, представителей, действующих на основании доверенности, и иных представителей контрагентов, с которыми у Общества существуют договорные отношения, с которыми Общество намерено вступить в договорные отношения или которые намерены вступить в договорные отношения с Обществом (далее – **Представители контрагентов**);
 - медицинских и фармацевтических работников, взаимодействующих с Обществом взаимодействующие с Обществом по вопросам обращения медицинских изделий, расходных материалов и продуктов, поставляемых и (или) предоставляемых Обществом (далее – **Медицинские и фармацевтические работники**);
 - специалистов сферы здравоохранения, представителей лечебно-профилактических учреждений, не являющихся медицинскими или фармацевтическими работниками, фармакоэкономистов, иных должностных лиц сферы здравоохранения (далее – **Специалисты здравоохранения**);
 - представителей организаций пациентов, благотворительных фондов, иных некоммерческих организаций в сфере здравоохранения, с которыми у Общества нет договорных отношений (далее – **Представители некоммерческих организаций**);
 - участников мероприятий в сфере здравоохранения, организуемых или спонсируемых Обществом (далее – **Участники мероприятий**);
 - потребителей, использующих медицинские изделия, расходные материалы и продукты поставляемых и (или) предоставляемых Обществом (в том числе направляющих запросы и претензии в отношении качества продукции) (далее – **Потребители**);
 - заявителей нежелательных явлений/информации по безопасности (далее – **Заявители НЯ**);
 - представителей субъектов персональных данных, не являющихся работниками Общества и обращающихся в Общество по поручению и от имени субъектов персональных данных (далее – **Представители субъектов**);
 - посетителей охраняемых помещений Общества, не имеющих права постоянного прохода в такие помещения (далее – **Посетители**);
 - авторизованных пользователей веб-сайтов Общества, заполнивших веб-формы регистрации (далее – **Пользователи сайтов**);
 - физических лиц, ставших участниками программы поддержки пациентов согласно правилам соответствующей программы (далее – **Участники программы**);
 - анонимных (неавторизованных) посетителей веб-сайтов Общества, в отношении которых обрабатывается информация, содержащаяся в файлах cookie, и сведения об IP-адресах (далее – **Посетители сайтов**).
- 2.2. Субъект персональных данных одновременно может относиться к нескольким категориям, указанным выше, например, являться Потребителем, Заявителем НЯ, Заявителем претензий и Посетителем сайтов и т. п.
- 2.3. Общество является лицом, осуществляющим предоставление персональных данных другим операторам в соответствии с требованиями законодательства, к которым относятся без ограничения:

- органы власти и местного самоуправления, государственные внебюджетные фонды, в которые перечисляются средства Обществом для зачисления на счета Работников (инспекции Федеральной налоговой службы, территориальные отделения Социального фонда России, Федерального фонда обязательного медицинского страхования и др.), надзорные органы;
- органы статистики, военные комиссариаты, операторы связи, иные организации, которым эта информация должна предоставляться в соответствии с законодательством РФ.

2.4. Органам власти, местного самоуправления и государственным внебюджетным фондам, органам статистики, военным комиссариатам, операторам связи и иным органам и организациям, указанным в пункте 3.2, персональные данные предоставляются (передаются) в объеме, определенном применимым законодательством, соответствующими органами власти и государственными внебюджетными фондами в пределах их полномочий. Согласие субъектов на такую передачу персональных данных не требуется.

3. Принципы обработки персональных данных

Обработка персональных данных Обществом осуществляется в соответствии со следующими принципами:

3.1. Законность и справедливая основа обработки персональных данных. Общество 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 определенных и законных целей. Целями обработки персональных данных Обществом являются:

- **в отношении Работников:**

- соблюдение трудового законодательства, включая выполнение возложенных законодательством на Общество как работодателя функций, полномочий и обязанностей, в частности, но не исчерпывая содействие в обучении и продвижение по службе, обеспечение личной безопасности работников, контроль количества и качества выполняемой работы, обеспечение сохранности имущества, расчет и выплата заработной платы, иных вознаграждений, расчет и перечисление налогов и отчислений, ведение воинского учета;
- предоставление Работникам дополнительных услуг за счет работодателя (предоставление средств корпоративной связи, перечисление доходов на платежные карты, страхование за счет работодателя, предоставление автомобиля и топливных карт, обеспечение командировок, оформление виз, разрешений на работу, приглашений на въезд в Россию и иностранные государства, оплата трансферов и пр.);

- **в отношении Работников компаний группы:** кадровое администрирование, корректный расчет заработной платы и вознаграждений;

- **в отношении Членов семей работников:**

- предоставление Работникам льгот и гарантий, предусмотренных законодательством и документами работодателя для лиц, имеющих (усыновивших) детей, лиц с семейными обязанностями, включая добровольное медицинское страхование Членов семей работников;

*Политика в отношении обработки персональных данных
и сведения о реализуемых требованиях к защите персональных данных*

- О выполнение требований Трудового кодекса РФ об информировании родственников о тяжелых несчастных случаях или несчастных случаях со смертельным исходом, выплата зарплаты в случае смерти работника;
- О выплата алиментов;
- **в отношении Руководителей и учредителей:** выполнение функций, полномочий и обязанностей, возложенных на Общество законодательством об обществах с ограниченной ответственностью (в том числе ведение списка участников Общества, проведение общего собрания участников Общества, проверка возможности совершения сделок, в том числе сделок с заинтересованностью и/или крупных сделок);
- **в отношении Соискателей:** принятие решения о возможности замещения вакантных должностей соискателями, наиболее полно соответствующими требованиям Общества; ведение кадрового резерва;
- **в отношении Представителей контрагентов:** выполнение норм Гражданского кодекса РФ, регулирующих договорную работу, заключение, включая проверку контрагентов, и исполнение договоров с контрагентами;
- **в отношении Медицинских и фармацевтических работников:** содействие в осуществлении медицинской деятельности, научное сотрудничество, информационное взаимодействие Общества с Медицинскими и фармацевтическими работниками по вопросам обращения медицинских изделий, расходных материалов и продуктов, поставляемых и (или) предоставляемых Обществом;
- **в отношении Специалистов здравоохранения и Представителей некоммерческих организаций:** информационное взаимодействие Общества со Специалистами здравоохранения и Представителями некоммерческих организаций по вопросам обращения медицинских изделий, расходных материалов и продуктов, поставляемых и (или) предоставляемых Обществом;
- **в отношении Участников мероприятий:** предоставление возможности участия в мероприятиях, организуемых или спонсируемых Обществом;
- **в отношении Потребителей:** информационное взаимодействие Общества с Потребителями, включая подготовку ответов на запросы Потребителей в отношении безопасности и качества медицинских изделий, расходных материалов и продуктов, поставляемых и(или) предоставляемых Обществом, рассмотрение претензий в отношении качества продукции;
- **в отношении Заявителей НЯ:** получение Обществом информации о нежелательных явлениях, информации по безопасности применения медицинских изделий, поставляемых и(или) предоставляемых Обществом;
- **в отношении Представителей субъектов:** выполнение Обществом действий по поручению Представителей субъектов персональных данных;
- **в отношении Посетителей:** обеспечение возможности прохода в охраняемые помещения Общества лиц, не имеющих постоянных пропусков, контроль их убытия;
- **в отношении Участников программы** - предоставление возможности участия в программах поддержки пациентов, организованных (спонсируемых) Обществом;
- **в отношении Пользователей сайтов:** предоставление возможности регистрации на сайтах Общества и использования предоставляемых сайтами сервисов;

- **в отношении Посетителей сайтов:** профилирование Посетителей веб-сайтов для облегчения навигации и учета индивидуальных предпочтений, получение статистических данных о посещении веб-сайтов.

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, несовместимой с целями сбора персональных данных, а также избыточных по отношению к заявленным целям обработки персональных данных. Общество не собирает и не обрабатывает персональные данные, не требующиеся для достижения целей, указанных в пункте 3.2 Политики, не использует персональные данные субъектов в каких-либо целях, кроме указанных.

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

3.5. Обеспечение точности, достаточности и актуальности персональных данных по отношению к целям обработки персональных данных. Общество принимает все разумные меры по поддержке актуальности обрабатываемых персональных данных, включая, но не ограничиваясь, реализацию права каждого субъекта получать для ознакомления свои персональные данные и требовать от Общества 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 без объяснения причин такого требования.

3.6. Хранение персональных данных 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, а также согласием субъекта персональных данных на обработку его персональных данных.

3.7. Уничтожение персональных данных по достижении заявленных целей их обработки или в случае утраты необходимости в достижении этих целей, при невозможности устранения Обществом допущенных нарушений установленного законодательством порядка обработки персональных данных, отзыве согласия на обработку субъектом персональных данных, выдвижения субъектом требования о прекращении обработки Обществом его персональных данных, истечении сроков обработки персональных данных, установленных локальными актами Общества, согласием на обработку персональных данных, если иное не предусмотрено законодательством или договорами с субъектами персональных данных, а носители персональных данных не подлежат передаче на архивное хранение.

3.8. При обработке персональных данных Общество исходит из того, что субъекты предоставляют достоверную информацию о себе и не принимают на себя каких-либо обязательств по проверке полученных персональных данных, хотя и оставляет за собой право при необходимости выполнить такую проверку законными способами.

4. Условия обработки персональных данных

4.1. Обработка персональных данных Обществом допускается в следующих случаях:

4.1.1. При наличии согласия субъекта персональных данных на обработку его персональных данных.

4.1.2. Обработка персональных данных необходима для достижения целей, предусмотренных законом, а также для осуществления и выполнения возложенных законодательством на Общество функций, полномочий и обязанностей.

4.1.3. Для заключения договора по инициативе субъекта персональных данных и исполнения договора, стороной которого или выгодоприобретателем по которому является или намеревается стать субъект персональных данных. Такими договорами, без ограничения, являются, трудовые договоры с Работниками, договоры страхования, в которых Работники и Члены семей работников являются выгодоприобретателями, договоры о сотрудничестве с Медицинскими и фармацевтическими работниками.

До момента заключения указанных договоров Общество осуществляет обработку персональных данных на стадии преддоговорной работы при подборе персонала, когда согласие субъекта на обработку подтверждается собственноручно заполненной анкетой Соискателя или анкетой (резюме), переданных им Обществу либо в специализированную организацию по подбору персонала, или размещенных Соискателем на специализированных веб-сайтах в сети Интернет, или направленных Соискателем Обществу по электронной почте. В случае, если заключение трудового договора иницируется Обществом, обработка персональных данных Соискателей ведется при наличии их согласия на обработку, полученного в любой доказываемой форме.

Договор, заключаемый с субъектом персональных данных, не может содержать положения, ограничивающие права и свободы субъекта персональных данных, устанавливающие случаи обработки персональных данных несовершеннолетних, если иное не предусмотрено законодательством Российской Федерации, а также положения, допускающие в качестве условия заключения договора бездействие субъекта персональных данных.

4.1.4. Обработка персональных данных необходима для осуществления прав и законных интересов Общества 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 путем дачи согласия на обработку персональных данных, разрешенных субъектом для распространения.

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

4.2. Общество не раскрывает третьим лицам и не распространяет персональные данные без согласия субъекта персональных данных, если иное не предусмотрено законодательством, договором с субъектом персональных данных, не указано в полученном от него согласии на обработку персональных данных.

4.3. Общество не обрабатывает персональные данные, относящиеся к специальным категориям и касающиеся расовой и национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни, состояния здоровья (за исключением сведений о состоянии здоровья Работников, связанных с возможностью выполнения Работником трудовой функции и необходимых для целей, определенных законодательством о государственной социальной помощи, законодательством об обязательных видах страхования, трудовым, пенсионным и страховым законодательством, а также сведений о состоянии здоровья Заявителей НЯ и Участников программы, связанных с использованием и предоставлением медицинских изделий, расходных материалов и продуктов, поставляемых и (или) предоставляемых Обществом), о членстве субъектов персональных данных в общественных объединениях или их профсоюзной деятельности, за исключением случаев, прямо предусмотренных законодательством.

4.4. Общество не обрабатывает персональные данные о судимости.

4.5. Общество не обрабатывает биометрические персональные данные.

4.6. При сборе персональных данных Общество обеспечивает запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных с использованием баз данных, находящихся на территории Общества и в дата-центрах на территории Российской Федерации.

4.7. Общество осуществляет трансграничную передачу персональных данных:

- Работников – в целях кадрового администрирования группы компаний Roche в соответствии с обязательными корпоративными правилами группы компаний на территорию Швейцарии, Венгрии, Ирландии, Нидерландов, Дании, Финляндии, Бельгии и иных государств, являющихся сторонами Конвенции Совета Европы ETS № 108 «О защите частных лиц в отношении автоматизированной обработки данных личного характера» и обеспечивающих адекватную защиту прав субъектов персональных данных;
- Медицинских и фармацевтических работников, Специалистов здравоохранения, Представителей некоммерческих организаций, Представителей контрагентов, Потребителей, Участников программы, Заявителей НЯ на территорию государств, являющихся сторонами Конвенции Совета Европы ETS № 108 «О защите частных лиц в отношении автоматизированной обработки данных личного характера» и обеспечивающих адекватную защиту прав субъектов персональных данных в целях:
 - организации взаимодействия, делового общения и научного сотрудничества в соответствии с корпоративной политикой группы компаний Roche и фиксации такого взаимодействия в информационной системе;
 - посещения компаний группы Roche, находящихся на территории иностранных государств, являющихся сторонами Конвенции Совета Европы ETS № 108 «О защите частных лиц в отношении автоматизированной обработки данных личного характера» и обеспечивающих адекватную защиту прав субъектов персональных данных;
 - выполнения регуляторных требований в области мониторинга безопасности медицинских изделий;
 - выполнения корпоративных правил группы компаний Roche в отношении централизации данных лиц, использующих медицинские изделия Roche, в информационной системе;
 - организации рассылки автоматических/полуавтоматических опросников удовлетворенности клиентов продуктами и услугами Roche и с целью аккумуляирования данных о клиентском опыте и удовлетворенности клиентов продукцией и услугами компании Roche для последующего анализа;
 - внутреннего контроля качества продукции и рассмотрения и учета обращений в глобальной системе компаний группы Roche.

4.8. Общество не принимает решения, порождающие юридические последствия в отношении субъектов персональных данных или иным образом затрагивающие их права и законные интересы, на основании исключительно автоматизированной обработки персональных данных. Данные, имеющие юридические последствия или затрагивающие права и законные интересы субъекта, подлежат перед их использованием проверке со стороны уполномоченного работника Общества.

5. Способы обработки персональных данных

5.1. Общество 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 в случаях, если такая 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) доступ к таким персональным данным.

6. Конфиденциальность персональных данных

6.1. Работниками Общества, получившими доступ к персональным данным, должна быть обеспечена конфиденциальность таких данных, за исключением сведений, в отношении которых субъектами даны согласия на их включение в общедоступные источники или распространение, а также персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

6.2. Общество 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 Общества, соблюдать принципы, правила обработки персональных данных и требования к их обработке, предусмотренные законодательством. Объем передаваемых другому лицу для обработки персональных данных, действия, выполняемые с персональными данными этим лицом, должны быть минимально необходимыми для выполнения им своих обязанностей перед Обществом.

В поручении Общества должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, цели обработки, перечень обрабатываемых по поручению персональных данных, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, по запросу Общества в течение срока действия поручения, в том числе до обработки персональных данных, предоставлять документы и иную информацию, подтверждающие принятие мер и соблюдение в целях исполнения поручения оператора требований, установленных статьей 6 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», об уведомлении Общества о фактах неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных, а также требования к защите обрабатываемых персональных данных в соответствии со статьей 19 указанного закона.

6.3. В случае, если Общество поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет Общество. Лицо, осуществляющее обработку персональных данных по поручению Общества, несет ответственность перед Обществом, за исключением иностранных лиц, осуществляющих обработку персональных данных по поручению Общества, которые несут ответственность перед субъектами персональных данных наряду с Обществом.

6.4. Общество вправе разместить свои информационные системы персональных данных в дата-центре (облачной вычислительной инфраструктуре). В этом случае в договор с дата-центром (провайдером облачных услуг) в качестве существенного условия может включаться

требование о запрете доступа персонала дата-центра (провайдера облачных услуг) к базам персональных данных Общества, размещаемых в дата-центре (облачной инфраструктуре), и тогда такое размещение не рассматривается Обществом как поручение обработки персональных данных дата-центру (провайдеру облачных услуг) и не требует согласия субъектов персональных данных на такое размещение.

7. Согласие субъекта персональных данных на обработку своих персональных данных

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

7.2. В случае получения Обществом персональных данных от контрагента на основании и в целях заключения и/или исполнения заключенного с ним договора, в том числе персональных данных работников от других компаний группы Roche, ответственность за правомерность предоставления персональных данных и их достоверность, а также за получение согласия Представителей контрагентов и Работников группы компаний на передачу их персональных данных Обществу и последующую обработку Обществом таких персональных данных несет контрагент, передающий персональные данные, что закрепляется в договоре с контрагентом.

7.3. Общество, получившее персональные данные от контрагента, не принимает на себя обязательства по информированию субъектов (их представителей), персональные данные которых ему переданы, о начале обработки персональных данных, поскольку обязанность осуществить соответствующее информирование при заключении договора с субъектом персональных данных и/или при получении согласия на такую передачу несет передавший персональные данные контрагент. Данная обязанность контрагента включается в договор, заключаемый с ним Обществом.

7.4. Специально 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, и для осуществления и выполнения возложенных законодательством на Общество функций, полномочий и обязанностей, за исключением случаев, когда необходимо получение письменного согласия Работника для конкретных случаев обработки персональных данных. К случаям, требующим письменного согласия Работника, относятся, не ограничиваясь:

7.4.1. Получение персональных данных Работников у третьих лиц, в том числе – с целью проверки таких персональных данных, а также в случаях, когда такие данные нельзя получить от самого Работника.

7.4.2. Передача персональных данных какой-либо третьей стороне, в том числе передача персональных данных контрагентам в целях заключения и исполнения договоров, участия в торгах, тендерах и т.д., при направлении в служебные командировки, на обучение и повышение квалификации, бронирования билетов, трансферов и гостиниц, оформления виз, разрешений на работу, приглашений на въезд в России и иностранные государства и т.п.

7.4.3. Передача персональных данных Работника третьим лицам в коммерческих целях, в том числе – банкам, открывающим и обслуживающим платежные карты для начисления заработной платы и иных доходов Работника, полиграфическим предприятиям,

занимающимся изготовлением визитных карточек (бизнес-карт) Работников за счет работодателя, организациям, занимающимся бронированием билетов и гостиниц и т.п.

7.4.4. Передача персональных данных Работника нотариусам для оформления нотариально заверяемых доверенностей от имени Общества и совершения иных нотариальных действий.

7.4.5. Передача персональных данных частной охранной организации с целью обеспечения прохода Работников в охраняемые помещения.

7.5. Специально выраженного согласия Членов семей работников не требуется, если обработка их персональных данных осуществляется на основании законодательства (для предоставления льгот и гарантий, оформления социальных выплат, начисления алиментов и пр.), выполняется Обществом как работодателем в соответствии с требованиями Трудового кодекса РФ, иных законов и нормативных правовых актов, а также в случаях, когда Члены семей работников являются выгодоприобретателями, в том числе – застрахованными лицами по договорам, заключенным Обществом как страховщиком в пользу Членов семей работников. Во всех остальных случаях необходимо получение доказываемого (подтверждаемого) согласия Членов семей работников на обработку их персональных данных Обществом.

7.6. Специально выраженного согласия Руководителей и учредителей на обработку их персональных данных не требуется, поскольку такая обработка необходима в целях выполнения возложенных на Общество законодательством об обществах с ограниченной ответственностью функций, полномочий и обязанностей.

7.7. Специально выраженного согласия Соискателей на обработку их персональных данных не требуется, поскольку такая обработка необходима в целях заключения трудовых договоров по инициативе Соискателей-субъектов персональных данных, за исключением случаев, когда необходимо получение согласия Соискателя в письменной форме для конкретных случаев обработки персональных данных. Персональные данные Соискателя, содержащиеся в его анкете, резюме, электронных письмах, направленных Обществу Соискателем или специализированными организациями по подбору персонала, и других документах, уничтожаются в течение 30 дней с даты принятия решения о приеме Соискателя на работу или об отказе в приеме на работу, за исключением Соискателей, выразивших согласие на включение во внешний кадровый резерв Общества. Персональные данные Соискателей, включенных во внешний кадровый резерв, хранятся в течение срока, указанного в согласии на обработку персональных данных и локальном акте Общества, регламентирующем ведение кадрового резерва.

В иных случаях, в том числе при обращении Общества к Соискателю с предложением о работе, для обработки персональных данных Соискателя необходимо получение его согласия на обработку персональных данных в любой доказываемой форме, например, в тексте анкеты, по электронной почте и т.д.

7.8. Персональные данные лиц, подписавших договоры с Обществом, и содержащиеся в единых государственных реестрах юридических лиц и индивидуальных предпринимателей, являются открытыми и общедоступными, за исключением сведений о номере, дате выдачи и органе, выдавшем документ, удостоверяющий личность физического лица. Обеспечение их конфиденциальности и согласие субъектов персональных данных на обработку таких данных не требуется.

Во всех остальных случаях необходимо получение согласия субъектов на обработку их персональных данных, являющихся Представителями контрагентов, за исключением лиц, подписавших договоры с Обществом, предоставивших доверенности на право действовать от имени и по поручению контрагентов Общества и тем самым совершивших конклюдентные действия, подтверждающие их согласие с обработкой персональных данных, указанных в

тексте договора (доверенности). Согласие Представителя контрагента на передачу его персональных данных Обществу и обработку им таких данных может получить контрагент в порядке, описанном в п.7.2 Политики. В этом случае получение Обществом согласия субъекта на обработку его персональных данных не требуется.

7.9. Медицинские и фармацевтические работники, Специалисты здравоохранения, Участники мероприятий и Участники программ, Представители некоммерческих организаций, Потребители дают свое согласие Обществу на обработку их персональных данных в любой доказываемой форме при предоставлении своих персональных данных, за исключением случаев, когда субъекты указанных в данном пункте категорий являются стороной договора с Обществом, который не требует получения согласия на обработку персональных данных.

7.10. Согласие Заявителей НЯ на обработку их персональных данных выражается в форме конклюдентных действий при обращении их в Общество и предоставлении своих персональных данных, за исключением обработки Обществом сведений о состоянии здоровья указанных лиц, которая осуществляется на основании согласия в письменной форме.

7.11. Согласие Представителей субъектов персональных данных на обработку их персональных данных выражается в форме конклюдентных действий путем предоставления доверенности с правом действовать от имени и по поручению субъектов персональных данных и документа, удостоверяющего личность Представителя субъекта персональных данных.

7.12. Согласие Посетителей на обработку их персональных данных дается в форме конклюдентных действий, а именно – предоставления документа, удостоверяющего личность, и сообщения сведений, запрашиваемых у него при посещении Общества.

7.13. Согласие Пользователей сайтов на обработку их персональных данных дается путем простановки соответствующей отметки в чек-боксе веб-формы на веб-сайте при заполнении ее персональными данными.

7.14. Согласие Посетителей сайта на обработку их персональных данных, получаемых Обществом и метрическим службами сети Интернет при просмотре Посетителями сайта страниц веб-сайта, дается путем принятия условий «Политики по работе с файлами cookies» и нажатии клавиши «Принять», «Согласен» или аналогичной клавиши, подтверждающей согласие в баннере, информирующем об использовании файлов cookies.

7.15. Равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе является согласие в форме электронного документа, подписанного электронной подписью в соответствии с законодательством об электронной подписи.

7.16. Согласие субъектов на предоставление их персональных данных не требуется при получении Обществом в рамках установленных полномочий мотивированных запросов от органов прокуратуры, правоохранительных органов, органов следствия и дознания, органов безопасности, от Росздравнадзора и государственных инспекторов труда и представителей при осуществлении ими своих функций 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.

7.17. В случае поступления запросов от организаций, не обладающих соответствующими полномочиями, Общество обязано получить от субъекта согласие 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 указанное правило будет (было) соблюдено. Порядок получения согласия Работников на передачу их персональных данных иным лицам описан в пункте 7.4 Политики.

7.18. Согласие на обработку персональных данных, обработка которых не установлена требованиями законодательства или не требуется для исполнения договора с Обществом, стороной которого является субъект персональных данных, может быть отозвано субъектом персональных данных. В этом случае Общество уничтожает такие персональные данные, в отношении которых отзывается согласие на обработку, и обеспечивает их уничтожение контрагентами, которым были переданы такие данные, в течение 30 календарных дней с момента получения отзыва согласия субъекта на обработку его персональных данных.

7.19. 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 Общество.

8. Права субъектов персональных данных

8.1. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных. Субъект персональных данных вправе требовать от Общества уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законодательством меры по защите своих прав.

8.2. Если субъект персональных данных считает, что Общество осуществляет обработку его персональных данных с нарушением требований законодательства или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие Общества в уполномоченный орган по защите прав субъектов персональных данных (Роскомнадзор) или в судебном порядке.

8.3. 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. Безопасность персональных данных, обрабатываемых Обществом, обеспечивается реализацией правовых, организационных и технических мер, необходимых и достаточных для обеспечения требований законодательства о персональных данных.

9.2. Правовые меры включают в себя:

- разработку локальных актов Общества, реализующих требования законодательства, в том числе Политики в отношении обработки персональных данных;
- отказ от любых способов обработки персональных данных, не соответствующих целям, заранее определенным Обществом.

9.3. Организационные меры включают себя:

- назначение лица, ответственного за организацию обработки персональных данных;
- назначение лица, ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных;

*Политика в отношении обработки персональных данных
и сведения о реализуемых требованиях к защите персональных данных*

- ограничение состава работников Общества, имеющих доступ к персональным данным, и организацию разрешительной системы доступа к ним;
- ознакомление работников Общества с положениями законодательства Российской Федерации о персональных данных, в том числе с требованиями к защите персональных данных, с Политикой, 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;
- проведение периодического внутреннего контроля (силами Общества) и аудита (с привлечением внешнего аудитора) соответствия обработки персональных данных требованиям законодательства, политике Общества в отношении обработки персональных данных и иным локальным актам Общества, регламентирующим работу с персональными данными с документальным оформлением результатов;
- определение в трудовых договорах и (или) должностных инструкциях работников Общества 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 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 требований к защите персональных данных при их обработке в информационных системах, исполнение которых обеспечивает установленные уровни защищенности персональных данных;
- 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 Общества, недопущение их нахождения в помещениях, где ведется работа с персональными данными и размещаются технические средства их обработки, без контроля со стороны работников Общества.

9.4. Технические меры включают в себя:

- 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, предусматривающей разграничение прав доступа пользователей;

- регистрацию и учёт действий с персональными данными пользователей информационных систем, где обрабатываются персональные данные;
- ограничение программной среды;
- выявление вредоносного программного обеспечения (применение антивирусных программ) на всех узлах информационной сети Общества, обеспечивающих соответствующую техническую возможность;
- безопасное межсетевое взаимодействие (применение межсетевого экранирования);
- идентификацию и проверку подлинности пользователя (аутентификацию) при входе в информационную систему по паролю;
- контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации;
- обнаружение фактов несанкционированного доступа к персональным данным и принятие мер, в том числе мер по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные системы персональных данных и по реагированию на компьютерные инциденты в них;
- принятие мер по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные системы персональных данных и по реагированию на компьютерные инциденты в них;
- защиту среды виртуализации;
- защиту сетевых устройств и каналов связи, по которым осуществляется передача персональных данных;
- восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним (система резервного копирования и восстановления персональных данных).

10. Заключительные положения

10.1. Иные обязанности и права Общества 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 Общества, виновные в нарушении норм, регулирующих обработку и защиту персональных данных, несут материальную, дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством.