

## Требования по защите Персональных данных

### 1. Применимость

Настоящие Требования по защите Персональных данных (далее – «Требования») являются частью Договора и включены в него посредством ссылки. Настоящие Требования и любое связанное с ним Соглашение о передаче данных будут оставаться в силе при истечении или прекращении действия Договора до тех пор, пока Персональные данные обрабатываются Поставщиком.

### 2. Определения

**«Персональные данные»** - любая информация, относящаяся к идентифицированному или идентифицируемому лицу, включая, без ограничений, данные на электронных и бумажных носителях, которые обрабатываются Поставщиком или лицами, привлекаемыми Поставщиком для исполнения обязательств по Договору, от имени и по указанию Novartis. Они могут включать в себя: имя или инициалы, домашний или другой адрес, номер телефона, фотографии и/или любые другие данные или информацию, подпадающую под действие Законов о защите данных.

**«Законы о защите данных»** - все законы, правила, или положения, касающиеся конфиденциальности, безопасности и/или целостности Персональных данных, которые применимы к работе Поставщика и Novartis, в том числе, но не ограничиваясь, Федеральным Законом от 27.07.2006 №152-ФЗ «О персональных данных».

**«Инцидент, связанный с обработкой Персональных данных»** - (а) потеря, непреднамеренное раскрытие, несанкционированный доступ к Персональным данным, а также к любым носителям, содержащим Персональные данные; (b) раскрытие или использование Персональных данных способом, не соответствующим Законам о защите данных, Договором или настоящими Требованиями; или (c) любые другие действия или упущения, которые отрицательно влияют на безопасность, конфиденциальность и/или целостность Персональных данных.

**«Субъект данных»** - идентифицированное или идентифицируемое лицо, чьи личные данные обрабатываются, получают, передаются, удаляются или хранятся Поставщиком от имени и по поручению Novartis. Идентифицированным лицом является тот, кто может быть идентифицирован, прямо или косвенно, в частности, путем использования идентификационного номера или одного или нескольких факторов, характерных для его физической, физиологической, умственной, экономической, культурной или социальной идентичности.

**«Обработка Персональных данных»** - любая обработка Персональных данных любыми способами, включая, без ограничений, сбор, доступ, получение, использование, передачу, извлечение, запись, организацию, хранение, сопровождение, хостинг, адаптацию, изменение, раскрытие (путем передачи, распространения или предоставления иным способом), блокирование, уничтожение или продажу.

**«Поставщик»** - Исполнитель и/или Поставщик Услуг по Договору, как он описан в Договоре.

**«Третьи лица, привлеченные для исполнения обязательств по Договору»** - любые третьи стороны, которые помогают Поставщику выполнять свои обязательства по Договору, включая аффилированных лиц и/или прямых или косвенных субподрядчиков Поставщика.

### 3. Информация об обрабатываемых Персональных данных

3.1 Сущность, цель предполагаемой обработки Персональных данных, перечень Персональных данных, категории субъектов Персональных данных определяются в Договоре.

#### **4. Технические и организационные меры по защите Персональных данных**

4.1 Поставщик должен осуществлять обработку Персональных данных исключительно в целях, указанных в Договоре и в прямом соответствии с указаниями Novartis. Все лица, имеющие доступ к Персональным данным, должны обеспечивать их конфиденциальность, ограничить их использование в конкретных целях. Доступ к Персональным данным должен осуществляться на основе необходимости и в объеме, достаточном для выполнения обязательств Поставщика. Поставщик обязан обеспечить, чтобы все лица, имеющие доступ к Персональным данным, получили надлежащую подготовку по вопросам обеспечения конфиденциальности и безопасности Персональных данных в соответствии с применимыми законами, правилами и промышленными стандартами, а также с правилами, определенными Novartis. Поставщик не должен использовать или раскрывать какие-либо Персональные данные, которые Поставщик создает, получает, обрабатывает или передает в результате выполнения своих обязательств, за исключением случаев, явно разрешенных или требуемых Договором.

4.2 Поставщик обеспечивает соблюдение минимальных технических и организационных мер по безопасности данных, указанных в Кодексе взаимодействия с третьими лицами Novartis, вместе с любыми дополнительными требованиями, если это применимо. Применимые технические и организационные меры зависят от технических особенностей обработки Персональных данных Поставщиком. В этой связи Поставщику разрешено применять альтернативные меры, которые позволяют обеспечить требуемый минимальный уровень безопасности данных. Существенные отличия от требований Novartis должны быть задокументированы.

4.3 В течение всего срока действия Договора Поставщик будет поддерживать работу собственной всеобъемлющей программы по обеспечению безопасности данных, которая включает политики и процедуры по защите данных, в соответствии с любыми договоренностями по конфиденциальности, установленными между сторонами, которые содержит административные, технические и физические способы защиты от разумно ожидаемых угроз безопасности, конфиденциальности или целостности, а также от угроз несанкционированной обработки Персональных данных. Поставщик будет периодически оценивать применимые риски по безопасности, конфиденциальности, целостности и устойчивости электронных, бумажных и других записей, содержащих Персональные данные, а также оценивать и повышать, при необходимости, эффективность своих средств защиты для снижения таких внутренних и внешних рисков.

#### **5. Корректировка, ограничение обработки и уничтожение Персональных данных**

5.1 Поставщик не может самостоятельно изменять, удалять или ограничивать обработку Персональных данных, обрабатываемых от имени Novartis, за исключением ситуаций, когда это предусмотрено письменными инструкциями от Novartis. Поставщик незамедлительно, но не позднее срока, определенного применимыми Законами о защите, уведомит Novartis в случае получения от субъекта Персональных данных любого запроса, имеющего отношение к соблюдению прав субъекта данных для обеспечения доступа или изменения Персональных данных, чтобы обеспечить следование всем инструкциям Novartis, регламентирующим работу с такими обращениями.

5.2 Права субъекта Персональных Данных на уничтожение, уточнение, предоставление Персональных данных, а также на доступ к ним должны обеспечиваться Поставщиком в соответствии с документально подтвержденными инструкциями от Novartis без неоправданной задержки.

5.3 При получении запроса на удаление персональных данных, обрабатываемых от имени Novartis, от Novartis, Поставщик обязан удалить персональные данные в соответствии требованиями законодательства РФ и предоставить Новартис подтверждение об удалении персональных данных в соответствии с Приказом Роскомнадзора от 28.10.2022 N 179 "Об утверждении Требований к подтверждению уничтожения персональных данных.

#### **6. Другие обязанности Поставщика**

6.1 Поставщик должен предоставить Novartis контактную информацию сотрудника, ответственного за обработку Персональных данных для организации прямого контакта между

сторонами. Novartis должен быть проинформирован в течение 24 (двадцати четырех) часов о любом изменении контактных данных такого сотрудника Поставщика.

6.2 Поставщик, как только это станет практически возможным, уведомляет Novartis в письменной форме о любом запросе в отношении Персональных данных (или доступа к ним), сделанным любым правительством, правоохранительным или регулирующим органом (но не позднее одного рабочего дня с даты такого запроса, если иное не следует из положений применимых Законов о защите данных), если такое уведомление Novartis не запрещено применимыми законами, правилами, положениями или постановлениями. Поставщик будет сотрудничать с Novartis в рамках подготовки ответов на такие запросы.

6.3 Novartis незамедлительно информируется о любых проверках (или других активностях), проводимых надзорными органами в отношении Поставщика, в случаях, если такие проверки относятся к обработке Персональных данных. В том числе это требование также применяется в случаях, когда Поставщик находится под следствием или является участником расследования, проводимого компетентным органом в связи с нарушениями какого-либо законодательства, а также административного правила или положения, касающегося обработки Персональных данных в связи с Договором.

## **7. Привлечение третьих лиц для исполнения обязательств по Договору**

7.1 Под привлечением третьих лиц в рамках настоящих Требований следует понимать привлечение третьих лиц для оказания услуг, которые непосредственно связаны с исполнением основного обязательства, направленного на обработку Персональных данных в соответствии с Договором. Такие действия не включают вспомогательные услуги, такие как телекоммуникационные услуги, почтовые/транспортные услуги, поддержку пользователей или уничтожение носителей данных, а также другие меры, направленные на обеспечение конфиденциальности, доступности, целостности и устойчивости аппаратного и программного обеспечения оборудования, используемого для обработки данных.

7.2 Поставщик понимает и соглашается с тем, что требования конфиденциальности и безопасности, содержащиеся в настоящих Требованиях, также без ограничения распространяются на любых третьих лиц, привлекаемых Поставщиком для исполнения обязательств по Договору, временных сотрудников или других лиц, которые получают Персональные данные в рамках Договора. С третьими лицами, привлекаемыми для исполнения обязательств по Договору, Поставщик должен заключать договоры, которые включают положения о защите Персональных данных, не менее ограничительные, чем положения, изложенные в настоящих Требованиях. По письменному запросу со стороны Novartis Поставщик обязуется предоставить копии таких договоров в течение семи рабочих дней. Novartis должно быть предоставлено (а) право контролировать и проверять привлекаемых Поставщиком третьих лиц, (б) право получать от Поставщика информацию о сущности взаимоотношения с такими третьими лицами и о соблюдении обязательств по защите данных в рамках таких взаимоотношений (по письменному запросу).

7.3 Если третье лицо, действующее по поручению Поставщика, обрабатывает Персональные данные за пределами Российской Федерации, Поставщик должен обеспечить соблюдение правил защиты данных, установленных в Российской Федерации а применимыми Законами о защите и/или соответствующими мерами, включая, без ограничений, выполнение требований Соглашения о передаче данных.

## **8. Инциденты, связанные с обработкой Персональных данных**

8.1 В любое время при обработке Персональных данных Поставщик незамедлительно, но не позднее 12 часов с момента обнаружения инцидента уведомляет Novartis о нарушении правил обработки Персональных данных, включая любое нарушение на объектах, системах или оборудовании лиц, привлеченных Поставщиком для обработки Персональных данных. Поставщик соглашается оказывать содействие и сотрудничать с Novartis в отношении информирования любых лиц, в том числе, регулирующих органов или субъектов Персональных данных, а также в отношении

принятия любых других мер по исправлению ситуации, если это необходимо в соответствии с любым применимым законом или следует из инструкций Novartis. Поставщик предпримет такие взаимно приемлемые шаги, чтобы исправить ситуацию и предотвратить повторение такого нарушения безопасности данных в будущем.

8.2 Если иное не требуется применимыми Законами о защите данных или любым другим законом, правилом, постановлением или предписанием, Поставщик не будет раскрывать информацию об инциденте с Персональными данными третьим сторонам или любым правительственным, правоохранительным или регулирующим органам, за исключением случаев, когда это предусмотрено договоренностью с Novartis или следует из положений применимых Законов о защите. Несмотря на вышесказанное, Поставщик может связаться с местной полицией в случае нарушения физической безопасности средств Поставщика или кражи оборудования или документов.

8.3 Поставщик за свой счет будет оказывать содействие и сотрудничать с Novartis в отношении предоставления информации об инцидентах, а также в отношении мер, направленных на устранение последствий инцидентов, если такое предоставление информации или меры запрашиваются со стороны Novartis или требуются законом, правилом, постановлением или положением, применимым к Поставщику или к Novartis, включая предоставление уведомления субъектам о нарушении безопасности их Персональных данных.

## **9. Уничтожение и возврат Персональных данных**

9.1 Копии или дубликаты записей с Персональными данными никогда не должны создаваться без уведомления Novartis, за исключением резервных копий, в случаях, когда это необходимо для обеспечения непрерывности обработки данных, если иное не предусмотрено нормативными требованиями и законами.

9.2 При прекращении или истечении срока действия Договора или в случае получения письменного запроса со стороны Novartis в любое время, Поставщик за свой счет и по выбору Novartis: (а) незамедлительно вернет все Персональные данные; или (б) уничтожит все документы, материалы и любые другие носители, которые могут содержать Персональные данные, без сохранения какой-либо части или копии. Поставщик предоставит Novartis подтверждение уничтожения Персональных данных в форме, приемлемой для Novartis, подписанной уполномоченным сотрудником Поставщика, который контролировал такое уничтожение.