

Статья I. Деловая контактная информация

Эта Статья применяется в том случае, если Поставщик или Kyndryl обрабатывает ДКИ другой стороны.

1.1 Kyndryl и Поставщик могут обрабатывать ДКИ другой стороны везде, где они ведут бизнес, в связи с предоставлением Поставщиком Услуг и Конечных продуктов.

1.2 Сторона:

(a) не будет использовать или раскрывать ДКИ другой стороны в любых других целях (для ясности, ни одна из сторон не будет продавать ДКИ другой стороны, использовать или раскрывать ДКИ другой стороны в любых маркетинговых целях без предварительного письменного согласия другой стороны и, если требуется, предварительного письменного согласия затронутых Субъектов персональных данных), а также

(b) будет удалять, изменять, исправлять, возвращать, предоставлять информацию об Обработке, ограничивать Обработку или предпринимать любые другие разумно запрашиваемые действия в отношении ДКИ другой стороны незамедлительно по письменному требованию другой стороны, когда происходит любое несанкционированное использование личной информации и сторона хочет прекратить обработку и осуществить исправление.

1.3 Стороны не вступают в совместную связь с Оператором персональных данных в отношении ДКИ друг друга, и никакие положения Документа о транзакции не должны интерпретироваться или толковаться как указывающие на намерение установить совместную связь с Оператором персональных данных.

1.4 Заявление о конфиденциальности Kyndryl, размещенное на <https://www.kyndryl.com/us/en/privacy>, содержит дополнительные сведения об Обработке ДКИ компанией Kyndryl.

1.5 Стороны внедрили и будут поддерживать технические и организационные меры безопасности для защиты ДКИ другой стороны от потери, уничтожения, изменения, случайного или несанкционированного раскрытия, случайного или несанкционированного доступа и незаконной Обработки.

1.6 Поставщик обязуется безотлагательно (и при любых обстоятельствах в пределах 48 часов) уведомлять Kyndryl о любых ставших ему известными случаях Нарушений безопасности в отношении ДКИ Kyndryl. Поставщик направляет такое уведомление по адресу cyber.incidents@kyndryl.com. Поставщик обязуется предоставлять Kyndryl по разумному запросу информацию о таких нарушениях безопасности и статусе любых действий Поставщика по устранению последствий и восстановлению работоспособности. Примером разумно запрошенной информации могут служить журналы привилегированного, административного и иного доступа к Устройствам, системам или приложениям, изображения Устройств, систем и приложений, сделанные в целях безопасности, и другие аналогичные материалы в объеме, в котором они имеют отношение к нарушению или к действиям Поставщика по устранению последствий и восстановлению работоспособности.

1.7 Если Поставщик обрабатывает только ДКИ Kyndryl и не имеет доступа к любым другим данным или материалам любого рода или к любой Корпоративной системе Kyndryl, данная Статья и Статья X (Сотрудничество, Проверка и Исправление) являются единственными Статьями, которые применяются к такой Обработке.

Статья II. Технические и организационные меры, Защита данных

Данная Статья применяется в том случае, если Поставщик обрабатывает Данные Kundryl, кроме ДКИ Kundryl. Поставщик обязуется отвечать требованиям настоящей Статьи при предоставлении всех Услуг и Конечных продуктов и таким образом защищать Данные Kundryl от потери, уничтожения, изменения, случайного или несанкционированного раскрытия, случайного или несанкционированного доступа и незаконных форм Обработки. Требования настоящей Статьи распространяются на все ИТ-приложения, платформы и инфраструктуру, эксплуатируемые или управляемые Поставщиком при предоставлении Конечных продуктов и Услуг, включая все среды разработки, тестирования, хостинга, поддержки, эксплуатации и центров обработки данных.

1. Использование данных

1.1 Поставщик не имеет права добавлять к Данным Kundryl или включать в Данные Kundryl любую другую информацию или данные, включая любые Персональные данные, без предварительного письменного согласия Kundryl, и не имеет права использовать Данные Kundryl в любой форме, агрегированной или иной, для любых целей, кроме предоставления Услуг и Конечных продуктов (например, Поставщику не разрешается использовать или повторно использовать Данные Kundryl для оценки эффективности средств улучшения предложений Поставщика, для исследований и разработок с целью создания новых предложений или для создания отчетов относительно предложений Поставщика). Если это прямо не разрешено в Документе о транзакции, Поставщику запрещается продавать Данные Kundryl.

1.2 Поставщик не встраивает технологии веб-отслеживания в Конечные продукты или как часть Услуг (такие технологии включают HTML5, локальную память, сторонние теги и веб-маяки), если это прямо не разрешено в Документе о транзакции.

2. Запросы третьих лиц и конфиденциальность

2.1 Поставщик не раскрывает Данные Kundryl третьим лицам, если только Kundryl не даст на это предварительное письменное разрешение. Если госсектор, включая любой регулятор, потребует доступ к Данным Kundryl (например, если правительство США направит Поставщику приказ по национальной безопасности о получении Данных Kundryl) или если раскрытие Данных Kundryl иным образом требуется по закону, Поставщик письменно уведомляет Kundryl о таком запросе или требовании и предоставляет Kundryl приемлемую возможность оспорить любое раскрытие (если закон запрещает уведомление, Поставщик предпримет шаги, которые он обоснованно считает необходимыми для оспаривания запрета и раскрытия Данных Kundryl в судебном порядке или иным способом).

2.2 Поставщик заверяет Kundryl, что: (a) только те его сотрудники, которым необходим доступ к Данным Kundryl для предоставления Услуг или Конечных продуктов, имеют такой доступ, и только в объеме, необходимом для предоставления этих Услуг и Конечных продуктов; и (b) он связал своих сотрудников обязательствами по соблюдению конфиденциальности, которые требуют от этих сотрудников использовать и раскрывать Данные Kundryl только в соответствии с настоящими Условиями.

3. Возврат или Удаление Данных Kundryl

3.1 Поставщик по выбору Kundryl либо удаляет, либо возвращает Kundryl Данные Kundryl после завершения или истечения срока действия Документа о транзакции или раньше по запросу Kundryl. Если Kundryl требует удаления, то Поставщик в соответствии с Передовой отраслевой практикой сделает данные нечитаемыми и не подлежащими повторной сборке или восстановлению и подтвердит удаление для Kundryl. Если Kundryl требует возврата Данных Kundryl, то Поставщик сделает это по разумному графику Kundryl и в соответствии с разумными письменными инструкциями Kundryl.

Статья III. Конфиденциальность

Эта Статья применяется в том случае, если Поставщик обрабатывает Персональные данные Kyndryl.

1. Обработка

1.1 Kyndryl назначает Поставщика Обработчиком Персональных данных Kyndryl исключительно в целях предоставления Конечных продуктов и Услуг в соответствии с инструкциями Kyndryl, в том числе содержащимися в настоящих Условиях, Документе о транзакции и связанном базовом соглашении между сторонами. Если Поставщик не выполняет инструкцию, Kyndryl может завершить затронутую часть Услуг по письменному уведомлению. Если Поставщик полагает, что инструкция нарушает закон о защите данных, Поставщик незамедлительно информирует об этом Kyndryl в сроки, предусмотренные законом. Если Поставщик не выполняет какое-либо из своих обязательств по настоящим Условиям и это невыполнение приводит к несанкционированному использованию Личной информации, или, в целом, в любом случае несанкционированного использования Личной информации Kyndryl имеет право остановить обработку, исправить невыполнение и устранить вредные последствия несанкционированного использования, при этом такое выполнение и устранение будут осуществляться по разумному указанию компании Kyndryl и в указанные ею разумные сроки.

1.2 Поставщик должен соблюдать все законы о защите данных, применимые к Услугам и Конечным продуктам.

1.3 Дополнение к Документу о транзакции или сам Документ о Транзакции устанавливает следующее в отношении Данных Kyndryl:

- (a) категории Субъектов персональных данных;
- (b) типы Персональных данных Kyndryl;
- (c) действия с данными и меры по Обработке;
- (d) продолжительность и частоту Обработки; и
- (e) список Подрядчиков Обработчика.

2. Технические и организационные меры

2.1 Поставщик реализует и поддерживает технические и организационные меры, изложенные в Статье II (Технические и организационные меры, Защита данных) и Статье VIII (Технические и организационные меры, Общая безопасность), и тем самым обеспечивает уровень безопасности, соответствующий риску, который представляют его Услуги и Конечные продукты. Поставщик подтверждает и понимает ограничения, изложенные в Статье II, настоящей Статье III и Статье VIII, и обязуется их соблюдать.

3. Права и Запросы Субъекта персональных данных

3.1 Поставщик немедленно информирует Kyndryl (в сроки, позволяющие Kyndryl и любым Другим Операторам персональных данных исполнять свои юридические обязательства) о любом запросе Субъекта персональных данных на осуществление любых прав Субъекта персональных данных (например исправление, удаление или блокирование данных) в отношении Персональных данных Kyndryl. Поставщик также может незамедлительно направить Субъекта персональных данных, делающего такой запрос, в Kyndryl. Поставщик не обязан давать ответ на запросы Субъектов персональных данных, если это не требуется по закону или если Kyndryl не даст письменное указание сделать это.

3.2 Если Kyndryl обязуется предоставить информацию относительно Персональных данных Kyndryl Другим Операторам персональных данных или другим третьим лицам (например Субъектам персональных данных или регуляторам), Поставщик должен помогать Kyndryl, предоставляя информацию и предпринимая другие разумные действия по требованию Kyndryl, в сроки,

позволяющие Kyndryl своевременно ответить таким Другим Операторам персональных данных или третьим лицам.

4. Подрядчики Обработчика

4.1 Поставщик заблаговременно направляет Kyndryl письменное уведомление перед добавлением нового Подрядчика Обработчика или расширением объема Обработки существующим Подрядчиком Обработчика, причем в таком письменном уведомлении будет указано имя Подрядчика Обработчика и описан новый или расширенный объем Обработки. Kyndryl может в любое время возразить против любого такого нового Подрядчика Обработчика или расширения объема на разумных основаниях, и если это произойдет, стороны совместно работают, основываясь на принципе добросовестности, над разрешением возражения Kyndryl. С учетом права Kyndryl на такое возражение в любое время, Поставщик может назначить нового Подрядчика Обработчика или расширить объем Обработки существующего Подрядчика Обработчика, если Kyndryl не высказала возражение в течение 30 Дней с даты направления письменного уведомления Поставщиком.

4.2 Поставщик обязуется накладывать обязательства по защите данных, их безопасности и сертификации, изложенные в настоящих Условиях, на каждого согласованного Подрядчика Обработчика до Обработки Подрядчиком Обработчика любых Данных Kyndryl. Поставщик несет полную ответственность перед Kyndryl за исполнение обязательств каждым Подрядчиком Обработчика.

5. Трансграничная Обработка Данных

Как указано ниже:

Страна, обеспечивающая адекватный уровень защиты, – страна, обеспечивающая адекватный уровень защиты данных в отношении соответствующей передачи в соответствии с применимым законом о защите данных или решениями регуляторов.

Импортер данных – либо Обработчик, либо Подрядчик Обработчика, который не зарегистрирован в Стране, обеспечивающей адекватный уровень защиты.

Стандартные договорные условия ЕС («СДУ ЕС») – Стандартные договорные условия ЕС (Решение Комиссии 2021/914) с применением необязательных условий, за исключением пункта 1 Условия 9(a) и пункта 2 Условия 17, официально опубликованных по адресу https://commission.europa.eu/publications/standard-contractual-clauses-international-transfers_en.

Стандартные договорные условия Сербии («СДУ Сербии») – Стандартные договорные условия Сербии, принятые «Уполномоченным Сербии по информации, имеющей общественное значение, и защите персональных данных», опубликованные по адресу <https://www.poverenik.rs/images/stories/dokumentacija-nova/podzakonski-akti/Klauzulelat.docx>.

Стандартные договорные условия («СДУ») – договорные условия, требуемые применимыми законами о защите данных для передачи Персональных данных Обработчикам, которые не имеют представительства в Странах, обеспечивающих адекватный уровень защиты.

Дополнение Соединенного Королевства по передаче данных за границу к Стандартным договорным условиям ЕС («Дополнение СК») – Дополнение Соединенного Королевства по передаче данных за границу к Стандартным договорным условиям ЕС, официально опубликованное по адресу <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-Transfer-agreement-and-guidance/>.

Дополнение Швейцарии к Стандартным договорным условиям ЕС («Швейцарское дополнение») означает договорные условия ЕС, применяемые в соответствии с решением Швейцарского органа по надзору за соблюдением законов о защите персональных данных (**FDPIC**) и в соответствии с Федеральным законом Швейцарии о защите данных (**FADP**).

5.1 Поставщик не должен передавать или раскрывать (в том числе посредством удаленного доступа) любые Персональные данные Kyndryl в разные страны, не получив предварительное письменное согласие Kyndryl. Если Kyndryl предоставляет такое согласие, стороны совместно работают над обеспечением соответствия требованиям применимых законов о защите данных. Если в соответствии с этими законами требуются СДУ, Поставщик незамедлительно заключает СДУ по запросу Kyndryl.

5.2 Относительно СДУ ЕС:

(a) Если у Поставщика нет представительства в Стране, обеспечивающей адекватный уровень защиты: Поставщик заключает СДУ ЕС в качестве Импортёра данных с Kyndryl, причем Поставщик обязуется заключить письменные соглашения со всеми одобренными Подрядчиками Обработчика в соответствии с Условием 9 СДУ ЕС и предоставить Kyndryl копии таких соглашений по запросу.

(i) Модуль 1 СДУ ЕС не применяется, если иное не согласовано сторонами в письменной форме.

(ii) Модуль 2 СДУ ЕС применяется, если Kyndryl является Оператором персональных данных, и Модуль 3 применяется, если Kyndryl является Обработчиком данных. В соответствии с Условием 13 СДУ ЕС, когда применяются Модули 2 или 3, стороны соглашаются, что (1) СДУ ЕС регулируются законом государства-участника ЕС, в котором располагается компетентный надзорный орган, и (2) любые споры, вытекающие из СДУ ЕС, подлежат рассмотрению в судах государства-участника ЕС, в котором располагается компетентный надзорный орган. Если такой закон в пункте (1) не разрешает прав стороннего бенефициара, то СДУ ЕС должны регулироваться законом Нидерландов, а любые споры, вытекающие из СДУ ЕС в соответствии с пунктом (2), разрешаются судом Амстердама в Нидерландах.

(b) Если у обеих сторон, Поставщика и Kyndryl, есть представительство в Стране, обеспечивающей адекватный уровень защиты, Поставщик действует в качестве Экспортёра данных и заключает СДУ ЕС со всеми одобренными Подрядчиками Обработчика в Стране, не обеспечивающей адекватный уровень защиты. Поставщик проводит требуемую Оценку воздействия передачи (ОВП) и без неоправданной задержки уведомляет Kyndryl о (1) необходимости применения дополнительных мер и (2) применяемых мерах. По запросу Поставщик предоставит Kyndryl результаты ОВП и любую информацию, необходимую для понимания и оценки результатов. В случае, если Kyndryl не согласна с результатами ОВП Поставщиков или примененными дополнительными мерами, Kyndryl и Поставщик вместе работают над поиском осуществимого решения. Kyndryl оставляет за собой право приостановить или завершить соответствующие услуги Поставщиков без компенсации. Во избежание сомнений, это не освобождает Подрядчиков Обработчика Поставщика от обязанности стать стороной СДУ ЕС с Kyndryl или ее Заказчиками, как указано в разделе 5.2 (d) ниже.

(c) Если Поставщик зарегистрирован в Европейской экономической зоне, а Kyndryl является Оператором персональных данных, на которого не распространяется действие Общоевропейского регламента о защите персональных данных (GDPR) 2016/679, то применяется Модуль 4 СДУ ЕС и Поставщик настоящим заключает с Kyndryl СДУ ЕС в качестве экспортёра данных. Если применяется Модуль 4 СДУ ЕС, стороны соглашаются, что СДУ ЕС должны регулироваться законом Нидерландов, а любые споры, вытекающие из СДУ ЕС, подлежат разрешению судом Амстердама в Нидерландах.

(d) Если Другие Операторы персональных данных, такие как Заказчики или филиалы, просят стать стороной СДУ ЕС в соответствии со «стыковочной оговоркой» в Условии 7, Поставщик настоящим соглашается на любой такой запрос.

(e) Технические и организационные меры, необходимые для выполнения Приложения II к СДУ ЕС, приведены в настоящих Условиях, самом Документе о транзакции и связанном базовом соглашении между сторонами.

(f) В случае противоречий между СДУ ЕС и настоящими Условиями преимущественной силой обладают СДУ ЕС.

5.3 В отношении Дополнения(-й) СК:

(a) Если у Поставщика нет представительства в Стране, обеспечивающей адекватный уровень защиты: (i) Поставщик заключает Дополнение(-я) СК с Kyndryl в качестве Импортёра данных в дополнение к СДУ ЕС, изложенным выше (если применимо, в зависимости от обстоятельств обработки); (ii) Поставщик обязуется заключить письменные соглашения со всеми одобренными Подрядчиками обработчика и предоставить Kyndryl копии таких соглашений по запросу.

(b) Если у Поставщика есть представительство в Стране, обеспечивающей адекватный уровень защиты, и Kyndryl является Оператором Персональных Данных, на которого не распространяется Общий регламент СК о защите персональных данных (вошедший в законодательство СК согласно Закону о выходе из Евросоюза от 2018 года), Поставщик заключает Дополнение(-я) СК с Kyndryl в качестве Экспортера данных в дополнение к СДУ ЕС, изложенным в разделе 5.2(b) выше.

(c) Если другие Операторы персональных данных, например Заказчики или аффилированные компании, потребуют заключения Дополнения(-й) СК, Поставщик обязуется удовлетворить такое требование.

(d) Информация, необходимая для заполнения Приложений (согласно Таблице 3) к Дополнению(-ям) СК, приводится в применимых СДУ ЕС, данных Положениях, в самом Документе по Транзакции и в соответствующем базовом соглашении между сторонами. Ни Kyndryl, ни Поставщик не могут расторгнуть Дополнение(-я) СК в случае внесения в него (них) каких-либо изменений.

(e) В случае противоречий между Дополнением(-ями) СК и данными Условиями преимущественную силу имеет(-ют) Дополнение(-я) СК.

5.4 В отношении СДУ Сербии:

(a) Если у Поставщика нет представительства в Стране, обеспечивающей адекватный уровень защиты: (i) Поставщик заключает СДУ Сербии с Kyndryl от имени Поставщика в качестве Обработчика данных; (ii) Поставщик обязуется заключить письменные соглашения со всеми одобренными Подрядчиками Обработчика в соответствии с СДУ Сербии и предоставить Kyndryl копии таких соглашений по запросу.

(b) Если у Поставщика есть представительство в Стране, обеспечивающей адекватный уровень защиты, Поставщик заключает СДУ Сербии с Kyndryl от имени всех Подрядчиков Обработчика, расположенных в Стране, не обеспечивающей адекватный уровень защиты. Если у Поставщика нет возможности сделать это для какого-либо такого Подрядчика Обработчика, Поставщик предоставляет Kyndryl СДУ Сербии, подписанные этим Подрядчиком Обработчика для скрепляющей подписи Kyndryl, прежде чем разрешить Подрядчику Обработчика обрабатывать любые Персональные данные Kyndryl.

(c) СДУ Сербии между Kyndryl и Поставщиком должны служить либо в качестве СДУ Сербии между Оператором персональных данных и Обработчиком данных, либо в качестве компенсационного соглашения в письменной форме между «Обработчиком данных» и «Подрядчиком Обработчика», как того требуют обстоятельства. В случае противоречий между СДУ Сербии и настоящими Условиями преимущественную силу имеют СДУ Сербии.

(d) Информация, необходимая для выполнения Приложений 1–8 к СДУ Сербии с целью регулирования переноса Персональных данных в Страну, не обеспечивающую адекватный уровень защиты, содержится в настоящих Условиях и в Дополнении к Документу о транзакции или в самом Документе о транзакции.

5.5. В отношении Дополнения(-й) Швейцарии:

(a) Если, и в той мере, в которой передача Kyndryl персональных данных в соответствии с разделом 5.1. регулируется Федеральным законом Швейцарии о защите данных (FADP), СДУ ЕС, согласованные в Разделе 5.2. настоящих Условий, будут регулировать эту передачу, с учетом следующих поправок в стандартных условиях GDPR для швейцарских персональных данных:

- Ссылки на Общеввропейский регламент о защите персональных данных (GDPR) следует понимать также как ссылки на эквивалентные положения FADP,
- Швейцарская федеральная комиссия по защите данных является компетентным надзорным органом согласно Статье 13 и Приложению I.C СДУ ЕС
- Швейцарское законодательство как регулирующее законодательство, если передача данных подлежит исключительно регулированию FADP, и
- Термин «государство-участник» в статье 18 СДУ ЕС должен также включать Швейцарию, чтобы позволить швейцарским субъектам данных осуществлять свои права по месту своего проживания.

(b) Во избежание сомнений, никакие из вышеперечисленных положений не должны снижать уровень защиты данных, предоставляемый СДУ ЕС, а только распространить этот уровень защиты на швейцарских субъектов данных. Если и в той мере, в какой это не имеет места, СДУ ЕС имеют преимущественную силу.

6. Помощь и Записи

6.1 Принимая во внимание характер Обработки, Поставщик помогает Kyndryl, принимая соответствующие технические и организационные меры по выполнению обязательств, относящихся к запросам и правам Субъекта персональных данных. Поставщик также помогает Kyndryl в обеспечении соблюдения обязательств, связанных с безопасностью Обработки, уведомлением и сообщением о Нарушении безопасности и разработкой оценок воздействия на защиту данных, включая предварительные консультации с ответственным регулятором, если потребуется, с учетом информации, доступной Поставщику.

6.2 Поставщик поддерживает актуальную запись имени и контактных данных каждого Подрядчика Обработчика, включая представителя каждого Подрядчика Обработчика и ответственного за защиту данных. Поставщик предоставляет Kyndryl эту запись в сроки, которые позволят Kyndryl своевременно отреагировать на любое требование Заказчика или другой третьей стороны.

Статья IV. Технические и организационные меры, Безопасность кода

Эта Статья применяется, если Поставщик получил доступ к Исходному коду Kyndryl. Поставщик обязуется соблюдать требования настоящей Статьи и тем самым защищать Исходный код Kyndryl от потери, уничтожения, изменения, случайного или несанкционированного раскрытия, случайного или несанкционированного получения доступа и незаконных форм Взаимодействия. Требования настоящей Статьи распространяются на все ИТ-приложения, платформы и инфраструктуру, эксплуатируемые или управляемые Поставщиком при предоставлении Конечных продуктов и Услуг и Взаимодействии с Технологией Kyndryl, включая все среды разработки, тестирования, хостинга, поддержки, эксплуатации и центров обработки данных.

1. Требования безопасности

Как указано ниже,

Запрещенная страна – любая страна: (а) определенная правительством США как враждебное иностранное государство в соответствии с Указом Президента США от 15 мая 2019 года «Об обеспечении безопасности цепочки поставок информационно-коммуникационных технологий и услуг», (б) указанная в соответствии с Разделом 1654 Закона об оборонном бюджете США от 2019 г., или (с) обозначенная как «Запрещенная страна» в Документе о транзакции.

1.1 Поставщик обязуется не распространять или помещать Исходный код Kyndryl в условное депонирование в интересах любой третьей стороны.

1.2 Поставщик не разрешает размещать Исходный код Kyndryl на серверах, расположенных в Запрещенной стране. Поставщик не разрешает никому, включая свой Персонал, пребывающий в Запрещенной стране или посещающий Запрещенную страну (в рамках любого такого посещения), по любой причине получать доступ или использовать любой Исходный код Kyndryl, независимо от того, где этот Исходный код Kyndryl находится в мире, причем Поставщик не разрешает проводить какие-либо разработки, тестирование или другие работы в Запрещенной стране, которые потребуют такого доступа или использования.

1.3 Поставщик обязуется не размещать и не распространять Исходный код Kyndryl в любой юрисдикции, где закон или толкование закона требует раскрытия Исходного кода любой третьей стороне. Если в юрисдикции, где находится Исходный код Kyndryl, произойдет изменение закона или толкования закона, которое может привести к обязательству Поставщика раскрыть такой Исходный код третьей стороне, Поставщик немедленно уничтожает или немедленно удаляет такой Исходный код Kyndryl из такой юрисдикции и обязуется не размещать дополнительный Исходный код Kyndryl в такой юрисдикции, если такой закон или толкование закона остается в силе.

1.4 Поставщик не должен прямо или косвенно предпринимать никаких действий, включая заключение любого соглашения, которое может привести к обязательству Поставщика, Kyndryl или любой третьей стороны по раскрытию информации согласно Разделам 1654 или 1655 Закона об оборонном бюджете США от 2019 г. Для ясности, за исключением случаев, когда это может быть прямо разрешено в Документе о транзакции или связанном базовом соглашении между сторонами, Поставщику не разрешается раскрывать Исходный код Kyndryl любой третьей стороне при любых обстоятельствах без предварительного письменного согласия Kyndryl.

1.5 Если Kyndryl уведомляет Поставщика или третья сторона уведомляет одну из сторон о том, что: (а) Поставщик допустил ввоз Исходного кода Kyndryl в Запрещенную страну или любую юрисдикцию, подпадающую под действие Раздела 1.3 выше, (б) Поставщик иным образом выпустил Исходный код Kyndryl, получил к нему доступ или использовал его способом, не разрешенным Документом о транзакции или связанным базовым или другим соглашением между сторонами, или (с) Поставщик нарушил Раздел 1.4 выше, то не ограничивая прав Kyndryl на устранение такого несоответствия по закону или по праву справедливости или в соответствии с Документом о транзакции или связанным базовым или другим соглашением между сторонами: (i) если такое уведомление направлено Поставщику, Поставщик незамедлительно передает уведомление Kyndryl; и (ii) Поставщик,

по разумному указанию Kyndryl, проводит расследование и выполняет исправление в сроки, которые Kyndryl разумно определит (после консультации с Поставщиком).

1.6 Если Kyndryl разумно полагает, что изменения в политике, процедурах, контроле или практике Поставщика в отношении доступа к Исходному коду могут быть необходимы для решения проблем кибербезопасности, кражи интеллектуальной собственности или аналогичных или связанных рисков (включая риск того, что без таких изменений Kyndryl может быть ограничена в продаже определенным Заказчикам или на определенные рынки или иным образом не сможет удовлетворить требования Заказчика по безопасности или цепочке поставок), то Kyndryl может связаться с Поставщиком для обсуждения действий, необходимых для устранения таких рисков, включая изменения в такой политике, процедурах, контроле или практике. По запросу Kyndryl Поставщик обязуется сотрудничать с Kyndryl по вопросам оценки необходимости таких изменений и внесения соответствующих взаимно согласованных изменений.

Статья V. Безопасная разработка

Настоящая Статья применяется в том случае, если Поставщик предоставляет Kyndryl свой или сторонний Исходный код или Локальное программное обеспечение или если любые из Конечных продуктов или Услуг Поставщика предоставлены Заказчику Kyndryl в составе продукта или услуги Kyndryl.

1. Готовность защиты

1.1 Поставщик взаимодействует с внутренними процессами Kyndryl, оценивающими готовность к защите продуктов и услуг Kyndryl, которые зависят от любого из Конечных продуктов Поставщика, включая своевременный и полный ответ на запросы о предоставлении информации, будь то документы, другие записи, интервью с соответствующим Персоналом Поставщика или тому подобное.

2. Безопасная разработка

2.1 Этот Раздел 2 применяется только в том случае, если Поставщик предоставляет Kyndryl Локальное программное обеспечение.

2.2 Поставщик реализовал и будет поддерживать в течение всего срока действия Документа о транзакции, в рамках Передовой отраслевой практики, политику, процедуры и средства контроля безопасности сети, платформы, системы, приложения, устройства, физической инфраструктуры, реагирования на инциденты и Персонала, которые необходимы для защиты: (а) систем и сред разработки, сборки, тестирования и эксплуатации, которые Поставщик или любая третья сторона, привлеченная Поставщиком, эксплуатирует, использует, и которыми она управляет или на которые полагается иным образом для или в отношении Конечных продуктов, а также (b) для защиты всего исходного кода Конечного продукта от потери, незаконных форм взаимодействия и несанкционированного доступа, раскрытия или изменения.

3. Сертификация по ISO 20243

3.1 Настоящий Раздел 3 применяется только в том случае, если любые Конечные продукты или Услуги Поставщика предоставляются Заказчику Kyndryl в составе продукта или услуги Kyndryl.

3.2 Поставщик получает сертификат соответствия стандартам ISO 20243, Информационные технологии, Open Trusted Technology Provider, Стандарт ТМ (O-TTPS), Защита от злонамеренно испорченных и поддельных продуктов (сертификат, полученный самостоятельно, либо основанный на оценке авторитетного независимого аудитора). В качестве альтернативы, если Поставщик запрашивает в письменной форме, а Kyndryl дает письменное согласие, Поставщик получает сертификат соответствия эквивалентному по существу отраслевому стандарту, касающемуся практик безопасной разработки и цепочки поставок (сертификат, полученный самостоятельно, либо основанный на оценке авторитетного независимого аудитора, по согласованию с Kyndryl).

3.3 Поставщик получает сертификат соответствия стандарту ISO 20243 или эквивалентному по существу отраслевому стандарту (по согласованию с Kyndryl в письменной форме) в течение 180 Дней после даты вступления в силу Документа о транзакции, а затем продлевает срок действия сертификата через каждые 12 месяцев (с каждым продлением срока действия на основе самой последней версии применимого стандарта, т. е. ISO 20243, или, по согласованию с Kyndryl в письменной форме, эквивалентного по существу отраслевого стандарта, касающегося практики безопасной разработки и цепочки поставок).

3.4 По запросу Поставщик незамедлительно предоставляет Kyndryl копию сертификатов, которые Поставщик обязан получить в соответствии с Разделами 2.1 и 2.2 выше.

4. Уязвимости защиты

Как указано ниже,

Исправление ошибок – исправления ошибок и пересмотры, которые устраняют ошибки или недостатки, включая Уязвимости защиты, в Конечных продуктах.

Функция защиты от сбоя – любые известные средства уменьшения или предотвращения рисков, связанных с Уязвимостью защиты.

Уязвимость защиты – состояние в проектировании, кодировании, разработке, реализации, тестировании, эксплуатации, поддержке, обслуживании или управлении Конечным продуктом, допускающее атаку любого лица, которая может привести к несанкционированному доступу или эксплуатации, включая: (а) доступ, контроль или нарушение работы системы, (b) доступ, удаление, изменение или извлечение данных или (с) изменение идентичности, полномочий или разрешений пользователей или администраторов. Уязвимость защиты может существовать независимо от того, присвоен ли ей идентификатор Common Vulnerabilities and Exposures (CVE) или любая оценка или официальная классификация.

4.1 Поставщик заявляет и гарантирует, что он будет: (а) использовать Передовую отраслевую практику для выявления Уязвимостей защиты, в том числе посредством постоянного статического и динамического сканирования безопасности приложений исходного кода, сканирования безопасности открытых источников и сканирования уязвимостей системы, и (b) соблюдать требования настоящих Условий, чтобы помочь предотвратить, обнаружить и устранить Уязвимости защиты в Конечных продуктах и во всех ИТ-приложениях, платформах и инфраструктуре, в которых Поставщик создает и предоставляет Услуги и Конечные продукты.

4.2 Если Поставщику становится известно об Уязвимости защиты в Конечном продукте или любом таком ИТ-приложении, платформе или инфраструктуре, Поставщик предоставляет Kyndryl Исправление ошибок и Функции защиты от сбоя для всех версий и релизов Конечных продуктов в соответствии с Уровнями серьезности и сроками, определенными в таблицах ниже:

Уровень серьезности*
Аварийная уязвимость защиты – это Уязвимость защиты, которая представляет собой серьезную и потенциально глобальную угрозу. Kyndryl определяет Аварийные уязвимости защиты по своему усмотрению, независимо от базового показателя CVSS.
Критическая — это Уязвимость защиты с базовым показателем CVSS от 9 до 10,0 баллов.
Высокая – это Уязвимость защиты с базовым показателем CVSS от 7,0 до 8,9 баллов.
Средняя – это Уязвимость защиты с базовым показателем CVSS от 4,0 до 6,9 баллов.
Низкая – это Уязвимость защиты с базовым показателем CVSS от 0,0 до 3,9 баллов.

Сроки				
<i>Аварийная</i>	<i>Критическая</i>	<i>Высокая</i>	<i>Средняя</i>	<i>Низкая</i>
<i>4 Дня или меньше, по решению начальника отдела информационной безопасности Kyndryl.</i>	30 Дней	30 Дней	90 Дней	Согласно Передовой отраслевой практике

* В любом случае, когда Уязвимость защиты не имеет четко определенного базового показателя CVSS, Поставщик применяет Уровень серьезности, соответствующий характеру и обстоятельствам такой уязвимости.

4.3 Для Уязвимости защиты, которая была публично раскрыта и для которой Поставщик еще не предоставил Kyndryl Исправление ошибок или Функции защиты от сбоя, Поставщик должен применять любые технически возможные дополнительные средства контроля безопасности, которые могут снизить риски, связанные с уязвимостью.

4.4 Если Kyndryl не удовлетворена ответом Поставщика на любую Уязвимость защиты в Конечном продукте или любом приложении, платформе или инфраструктуре, упомянутых выше, то без ущерба для любых других прав Kyndryl Поставщик незамедлительно организует для Kyndryl обсуждение ее проблем непосредственно с вице-президентом Поставщика или эквивалентным руководителем, ответственным за предоставление Исправления ошибок.

4.5 Примеры Уязвимостей защиты включают в себя сторонний код или открытый исходный код, вышедший из эксплуатации (EOS), когда эти типы кода больше не получают исправлений защиты.

Статья VI. Доступ к корпоративным системам

Настоящая Статья применяется, если у сотрудников Поставщика есть доступ к любой Корпоративной системе.

1. Общие условия

1.1 Kyndryl определяет, разрешать ли сотрудникам Поставщика доступ к Корпоративным системам. Если Kyndryl предоставляет такое разрешение, Поставщик обязуется соблюдать и требует от своих сотрудников, имеющих такой доступ, соблюдать требования настоящей Статьи.

1.2 Kyndryl определяет средства, с помощью которых сотрудники Поставщика могут получить доступ к Корпоративным системам, включая то, будут ли такие сотрудники получать доступ к Корпоративным системам через Устройства, предоставленные Kyndryl или Поставщиком.

1.3 Сотрудники Поставщика могут получать доступ к Корпоративным системам и использовать только те Устройства, которые Kyndryl разрешает в целях такого доступа, для предоставления Услуг. Сотрудники Поставщика не имеют права использовать Устройства, которые Kyndryl разрешает для предоставления услуг любому другому физическому или юридическому лицу или для доступа к любым ИТ-системам, сетям, приложениям, веб-сайтам, средствам электронной почты, средствам совместной работы Поставщика или третьих лиц для предоставления Услуг или в связи с ними.

1.4 Для ясности, сотрудники Поставщика не имеют права использовать Устройства, которые Kyndryl разрешает для доступа к Корпоративным системам, в личных целях (например, сотрудники Поставщика не имеют права хранить личные файлы, такие как музыка, видео, фотографии или другие подобные элементы на таких Устройствах и не могут пользоваться Интернетом с таких Устройств в личных целях).

1.5 Сотрудники Поставщика не должны копировать Материалы Kyndryl, доступные через Корпоративную систему, без предварительного письменного разрешения Kyndryl (и никогда не должны копировать Материалы Kyndryl на портативные устройства хранения, такие как USB, внешний жесткий диск или другие подобные устройства).

1.6 По запросу Поставщик подтверждает, по имени сотрудника, конкретные Корпоративные системы, к которым его сотрудникам разрешается иметь доступ, и доступ к которым они получили за любой период времени, указанный Kyndryl.

1.7 Поставщик уведомляет Kyndryl в течение 24 (двадцати четырех) часов после того, как любой сотрудник Поставщика, имеющий доступ к любой Корпоративной системе, перестанет: (а) работать на Поставщика или (б) заниматься деятельностью, требующей такого доступа. Поставщик сотрудничает с Kyndryl для обеспечения немедленного аннулирования доступа для таких бывших или нынешних сотрудников.

1.8 Поставщик немедленно сообщает Kyndryl о любых фактических или предполагаемых инцидентах, связанных с нарушением безопасности (таких как потеря Устройства Kyndryl или Поставщика или несанкционированный доступ к Устройству или данным, материалам или другой информации любого рода) и сотрудничает с Kyndryl над расследованием таких инцидентов.

1.9 Поставщик не имеет права разрешать любому агенту, независимому подрядчику или сотруднику субподрядчика получать доступ к любой Корпоративной системе без предварительного письменного согласия Kyndryl; если Kyndryl дает такое согласие, то Поставщик по договору обязует этих лиц и их работодателей соблюдать требования настоящей Статьи, как если бы эти лица были сотрудниками Поставщика, и несет ответственность перед Kyndryl за все действия и бездействие любого такого лица или работодателя в отношении такого доступа к Корпоративной системе.

2. Программное обеспечение Устройства

2.1 Поставщик поручает своим сотрудникам своевременно установить все программное обеспечение Устройства, которое требуется Kyndryl для обеспечения безопасного доступа к Корпоративным системам. Ни Поставщик, ни его сотрудники не должны вмешиваться в работу этого программного обеспечения или в функции защиты, которые обеспечивает программное обеспечение.

2.2 Поставщик и его сотрудники придерживаются правил конфигурирования Устройства, которые устанавливает Kyndryl, и иным образом работают совместно с Kyndryl над обеспечением функционирования программного обеспечения в соответствии с намерениями Kyndryl. Например, Поставщик не должен отменять блокировку веб-сайтов программного обеспечения или функции автоматического исправления.

2.3 Сотрудники Поставщика не имеют права передавать Устройства, которые они используют для доступа к Корпоративным системам, или имена пользователей Устройств, их пароли и тому подобное другим лицам.

2.4 Если Kyndryl разрешает сотрудникам Поставщика получать доступ к Корпоративным системам с помощью Устройств Поставщика, то Поставщик установит и запустит операционную систему на этих Устройствах, которую одобрит Kyndryl, и обновит ее до новой версии или новой операционной системы в течение разумного времени после того, как Kyndryl даст соответствующие указания.

3. Надзор и Сотрудничество

3.1 Kyndryl имеет безоговорочное право контролировать и устранять потенциальные вторжения и другие угрозы кибербезопасности любыми способами, из любых мест и с использованием любых средств, которые Kyndryl считает необходимыми или подходящими, без предварительного уведомления Поставщика или любого сотрудника Поставщика или других лиц. В качестве примера таких прав Kyndryl может в любое время: (а) провести тест защиты на любом Устройстве, (б) контролировать, восстанавливать с помощью технических или иных средств и просматривать сообщения (включая электронные сообщения с любых учетных записей электронной почты), записи, файлы и другие элементы, хранящиеся на любом Устройстве или передаваемые через любую Корпоративную систему, и (с) получить полный криминалистический образ любого Устройства. Если Kyndryl нуждается в сотрудничестве с Поставщиком для осуществления своих прав, Поставщик будет полностью и своевременно удовлетворять запросы Kyndryl о таком сотрудничестве (включая, например, запросы на безопасное конфигурирование любого Устройства, установку мониторингового или другого программного обеспечения на любом Устройстве, обмен данными о подключении на системном уровне, участие в мерах реагирования на инциденты на любом Устройстве, предоставление физического доступа к любому Устройству для Kyndryl с целью получения полного криминалистического образа или иным образом, а также аналогичные и связанные запросы).

3.2 Kyndryl может отозвать доступ к Корпоративным системам в любое время, для любого сотрудника Поставщика или всех сотрудников Поставщика, без предварительного уведомления Поставщика или любого сотрудника Поставщика или других лиц, если Kyndryl считает, что это необходимо для защиты Kyndryl.

3.3 Права Kyndryl не блокируются, не уменьшаются и не ограничиваются каким-либо образом любым положением Документа о транзакции, связанного базового соглашения между сторонами или любого другого соглашения между сторонами, включая любое положение, которое может требовать, чтобы данные, материалы или другая информация любого рода находились только в выбранном месте или местах, или которое может требовать, чтобы только лица из выбранного места или мест имели доступ к таким данным, материалам или другой информации.

4. Устройства Kyndryl

4.1 Kyndryl сохраняет право собственности на все Устройства Kyndryl, при этом Поставщик несет риск потери Устройств, в том числе в результате кражи, вандализма или неосторожности. Поставщик не должен вносить или разрешать вносить любые изменения в Устройства Kyndryl без предварительного письменного согласия Kyndryl, при этом изменением считается любое изменение Устройства, включая любое изменение программного обеспечения, приложений, схемы безопасности, конфигурации защиты, физической, механической или электрической конструкции Устройства.

4.2 Поставщик обязуется вернуть все Устройства Kyndryl в течение 5 рабочих дней после прекращения необходимости использования этих Устройств для оказания Услуг и, если Kyndryl потребует, должен одновременно уничтожить все данные, материалы и другую информацию любого рода на этих Устройствах, не сохраняя никаких копий, следуя Передовой отраслевой практике для окончательного стирания всех таких данных, материалов и другой информации. Поставщик за свой счет упаковывает и возвращает Устройства Kyndryl в том же состоянии, в котором они были доставлены Поставщику, за исключением разумного износа, в место, которое определяет Kyndryl. Несоблюдение Поставщиком любого обязательства в настоящем Разделе 4.2 является существенным нарушением Документа о транзакции и связанного базового соглашения и любого связанного соглашения между сторонами при том понимании, что соглашение является «связанным», если доступ к любой Корпоративной системе облегчает задачи Поставщика или другие действия по этому соглашению.

4.3 Kyndryl обеспечивает поддержку Устройств Kyndryl (включая проверку Устройства и профилактическое и восстановительное обслуживание). Поставщик немедленно уведомляет Kyndryl о необходимости проведения ремонтных работ.

4.4. Для программного обеспечения, которым владеет компания Kyndryl или на которое она имеет право выдавать лицензию, Kyndryl предоставляет Поставщику временное право использовать, хранить и делать достаточное число копий для поддержки санкционированного использования Устройств Kyndryl. Поставщик не имеет права передавать программы кому-либо, делать копии информации о лицензиях на программное обеспечение, а также дизассемблировать, декомпилировать, выполнять обратную разработку или иным образом преобразовывать любую программу, если это прямо не разрешено применимым законом без возможности отказа от исполнения договорных обязательств.

5. Обновления

5.1 Невзирая на какие-либо положения об обратном в Документе о транзакции или связанном базовом соглашении между сторонами, после письменного уведомления Поставщика и без необходимости получения его согласия Kyndryl может обновлять, дополнять или иным образом изменять данную Статью для выполнения любого требования применимого закона или обязательства Заказчика, для отражения любой разработки в передовых практиках безопасности или иным образом, как Kyndryl считает необходимым для защиты Корпоративных систем или Kyndryl.

Статья VII. Набор персонала

Данная Статья применяется в том случае, если сотрудники Поставщика посвящают все свое рабочее время предоставлению Услуг для Kyndryl, выполняя все эти Услуги в комплексе помещений Kyndryl, комплексе помещений Заказчика или из своего дома и предоставляя Услуги только с использованием Устройств Kyndryl для получения доступа к Корпоративным системам.

1. Доступ к Корпоративным системам; Среды Kyndryl

1.1 Поставщик может выполнять Услуги только путем доступа к Корпоративным системам с использованием Устройств, которые предоставляет Kyndryl.

1.2 Поставщик должен соблюдать условия, изложенные в Статье VI (Доступ к Корпоративным системам), в отношении всего объема доступа к Корпоративным системам.

1.3 Устройства, предоставленные Kyndryl, являются единственными Устройствами, которые Поставщик и его сотрудники могут использовать для оказания Услуг, и могут использоваться только Поставщиком и его сотрудниками для оказания Услуг. Для ясности, ни при каких обстоятельствах Поставщик или его сотрудники не могут использовать другие устройства для предоставления Услуг или использовать Устройства Kyndryl для любого другого заказчика Поставщика или для любой другой цели, кроме предоставления Услуг для Kyndryl.

1.4 Сотрудники Поставщика, использующие Устройства Kyndryl, могут передавать Материалы Kyndryl друг другу и хранить такие материалы на Устройствах Kyndryl, но только в той ограниченной степени, в которой такой обмен и хранение необходимы для успешного выполнения Услуг.

1.5 За исключением такого хранения на Устройствах Kyndryl, Поставщик или его сотрудники ни при каких обстоятельствах не имеют права удалять любые Материалы Kyndryl из хранилищ, сред, инструментов или инфраструктуры Kyndryl, где их хранит Kyndryl.

1.6 Для ясности, Поставщик и его сотрудники не имеют права передавать какие-либо Материалы Kyndryl в какие-либо хранилища, среды, инструменты или инфраструктуру Поставщика или любые другие системы, платформы, сети Поставщика без предварительного письменного согласия Kyndryl.

1.7 Статья VIII (Технические и организационные меры, Общая безопасность) не применяется к Услугам Поставщика, если сотрудники Поставщика посвящают все свое рабочее время предоставлению Услуг для Kyndryl, выполняя все эти Услуги в комплексе помещений Kyndryl, в комплексе помещений Заказчика или из своего дома, и предоставляют Услуги только с использованием Устройств Kyndryl для доступа к Корпоративным системам. В противном случае к Услугам Поставщика применяется Статья VIII.

Статья VIII. Технические и организационные меры, Общая безопасность

Данная Статья применяется в том случае, если Поставщик предоставляет Kyndryl Услуги или Конечные продукты, за исключением случаев, когда у Поставщика есть доступ только к ДКИ Kyndryl при предоставлении этих Услуг и Конечных продуктов (т. е. Поставщик не должен обрабатывать другие Данные Kyndryl или иметь доступ к другим Материалам Kyndryl или к Корпоративной системе), при этом единственными Услугами и Конечными продуктами Поставщика является предоставление Kyndryl Локального программного обеспечения, или Поставщик предоставляет все свои Услуги и Конечные продукты в модели набора персонала в соответствии со Статьей VII, включая Раздел 1.7 указанной Статьи.

Поставщик обязуется соблюдать требования настоящей Статьи и тем самым защищать: (а) Материалы Kyndryl от потери, уничтожения, изменения, случайного или несанкционированного раскрытия, случайного или несанкционированного доступа, (б) Данные Kyndryl – от незаконных форм Обработки и (с) Технологии Kyndryl – от незаконных форм Взаимодействия. Требования настоящей Статьи распространяются на все ИТ-приложения, платформы и инфраструктуру, эксплуатируемые или управляемые Поставщиком при предоставлении Конечных продуктов и Услуг и Взаимодействии с Технологией Kyndryl, включая все среды разработки, тестирования, хостинга, поддержки, эксплуатации и центров обработки данных.

1. Политика в области безопасности

1.1 Поставщик обязуется поддерживать и соблюдать политики и практики в области ИТ-безопасности, которые являются неотъемлемой частью бизнеса Поставщика, обязательны для всего Персонала Поставщика и соответствуют Передовой отраслевой практике.

1.2 Поставщик должен пересматривать свои политики и практики в области ИТ-безопасности не реже одного раза в год и вносить в них изменения, которые Поставщик сочтет необходимыми для защиты Материалов Kyndryl.

1.3 Поставщик обязуется поддерживать и соблюдать стандартные, обязательные требования по проверке при трудоустройстве всех новых сотрудников и распространять такие требования на весь Персонал Поставщика и дочерние компании Поставщика, находящиеся в полной собственности. Эти требования должны включать проверку на наличие правонарушений в той степени, в которой это разрешено местным законодательством, проверку удостоверения личности и дополнительные проверки, которые Поставщик сочтет необходимыми. Поставщик периодически проверяет и перепроверяет эти требования, если сочтет необходимым.

1.4 Поставщик ежегодно проводит обучение своих сотрудников по вопросам безопасности и конфиденциальности и требует от всех таких сотрудников ежегодного подтверждения того, что они будут соблюдать этические нормы ведения бизнеса, политики в области конфиденциальности и безопасности Поставщика, изложенные в кодексе поведения Поставщика или в аналогичных документах. Поставщик обеспечивает дополнительное обучение политике и процессам для лиц, имеющих административный доступ к любым компонентам Услуг, Конечным продуктам или Материалам Kyndryl, причем такое обучение зависит от их роли и поддержки Услуг, Конечных продуктов и Материалов Kyndryl и необходимо для поддержания требуемого соответствия и сертификации.

1.5 Поставщик разрабатывает меры безопасности и конфиденциальности для защиты и поддержания доступности Материалов Kyndryl, в том числе путем реализации, поддержания и соблюдения политик и процедур, требующих обеспечения безопасности и конфиденциальности путем проектирования, безопасного инжиниринга и безопасной эксплуатации, для всех Услуг и Конечных продуктов и для всех Взаимодействий с Технологией Kyndryl.

2. Инциденты, связанные с нарушением безопасности

2.1 Поставщик поддерживает и соблюдает задокументированную политику реагирования на инциденты, связанные с нарушением безопасности, соответствующую Передовой отраслевой практике по разрешению инцидентов, связанных с нарушением компьютерной безопасности.

2.2 Поставщик расследует случаи несанкционированного доступа или несанкционированного использования Материалов Kyndryl, определяет и выполняет соответствующий план реагирования.

2.3 Поставщик обязуется безотлагательно (и при любых обстоятельствах в пределах 48 часов) уведомлять Kyndryl о любых ставших ему известными случаях Нарушений безопасности. Поставщик направляет такое уведомление по адресу cyber.incidents@kyndryl.com. Поставщик обязуется предоставлять Kyndryl по разумному запросу информацию о таких нарушениях безопасности и статусе любых действий Поставщика по устранению последствий и восстановлению работоспособности. Примером разумно запрошенной информации могут служить журналы привилегированного, административного и иного доступа к Устройствам, системам или приложениям, изображения Устройств, систем и приложений, сделанные в целях безопасности, и другие аналогичные материалы в объеме, в котором они имеют отношение к нарушению или к действиям Поставщика по устранению последствий и восстановлению работоспособности.

2.4 Поставщик предоставляет Kyndryl разумную помощь для выполнения любых юридических обязательств (включая обязательства по уведомлению регуляторов или Субъектов персональных данных) Kyndryl, филиалов Kyndryl и Заказчиков (и их заказчиков и филиалов) в связи с Нарушением безопасности.

2.5 Поставщик не должен информировать или уведомлять любую третью сторону о том, что Нарушение безопасности прямо или косвенно связано с Kyndryl или Материалами Kyndryl, если Kyndryl не одобрит это в письменной форме или если это не требуется по закону. Поставщик уведомляет Kyndryl в письменной форме до направления любого законного уведомления третьей стороне, если такое уведомление прямо или косвенно раскрывает идентичность Kyndryl.

2.6 В случае Нарушения безопасности, возникшего в результате нарушения Поставщиком любого обязательства по настоящим Условиям:

(a) Поставщик должен нести ответственность за любые расходы, которые он понесет, а также фактические расходы, которые понесет Kyndryl, при направлении уведомления о Нарушении безопасности применимым регуляторам, другим государственным и соответствующим отраслевым саморегулируемым агентствам, средствам массовой информации (если это требуется применимым законодательством), Субъектам персональных данных, Заказчикам и другим лицам;

(b) по требованию Kyndryl Поставщик обязуется создать и содержать за свой счет колл-центр для ответов на вопросы Субъектов персональных данных о Нарушении безопасности и его последствиях в течение 1 года после даты уведомления таких Субъектов персональных данных о Нарушении безопасности или в соответствии с требованиями любого применимого закона о защите данных, в зависимости от того, что обеспечивает большую защиту. Kyndryl и Поставщик вместе работают над созданием сценариев и других материалов, которые будут использоваться сотрудниками колл-центра при ответе на запросы. В качестве альтернативы, по письменному уведомлению Поставщика, Kyndryl может создать и поддерживать свой собственный колл-центр вместо того, чтобы Поставщик создавал колл-центр, и Поставщик возместит Kyndryl фактические расходы, которые Kyndryl понесет при создании и поддержании такого колл-центра, и

(c) Поставщик должен возместить Kyndryl фактические расходы, которые Kyndryl понесет при предоставлении услуг кредитного мониторинга и восстановления кредитоспособности в течение 1 года после даты предоставления уведомления о Нарушении безопасности лицам, пострадавшим от нарушения, решившим зарегистрироваться для получения таких услуг, или в соответствии с требованиями любого применимого закона о защите данных, в зависимости от того, что обеспечивает большую защиту.

3. Физическая безопасность и Контроль входа (как указано ниже, «Объект» – это физическое место, в котором Поставщик размещает, обрабатывает или иным образом получает доступ к Материалам Kyndryl).

3.1 Поставщик обязуется поддерживать соответствующие физические средства контроля входа, такие как барьеры, пункты входа, управляемые карточками, камеры наблюдения и стойки приема посетителей, для защиты от несанкционированного входа на Объекты.

3.2 Поставщик должен требовать авторизованного разрешения на доступ к Объектам и контролируемым зонам в пределах Объектов, включая любой временный доступ, и ограничивать доступ по роли задания и потребности бизнеса. Если Поставщик предоставляет временный доступ, его уполномоченный сотрудник будет сопровождать любого посетителя во время нахождения на территории Объекта и в любых контролируемых зонах.

3.3 Поставщик применяет средства контроля физического доступа, включая многофакторные средства контроля доступа, соответствующие Передовой отраслевой практике, для надлежащего ограничения доступа в контролируемые зоны Объектов, регистрирует все попытки входа и хранит такие журналы в течение не менее одного года.

3.4 Поставщик аннулирует доступ к Объектам и контролируемым зонам в пределах Объектов (a) после увольнения уполномоченного сотрудника Поставщика или (b) если уполномоченный сотрудник Поставщика больше не имеет действительной бизнес-потребности в доступе. Поставщик соблюдает формальные задокументированные процедуры увольнения, которые включают оперативное удаление из списков контроля доступа и сдачу пропусков физического доступа.

3.5 Поставщик принимает меры предосторожности для защиты всей физической инфраструктуры, используемой для поддержки Услуг и Конечных продуктов и Взаимодействия с Технологией Kyndryl, от угроз окружающей среды, как естественных, так и антропогенных, таких как повышенная температура окружающей среды, пожар, наводнение, влажность, кража и вандализм.

4. Доступ, Вмешательство, Передача и Управление разделением

4.1 Поставщик поддерживает задокументированную архитектуру безопасности сетей, которыми он управляет при оказании Услуг, предоставлении Конечных продуктов и Взаимодействии с Технологией Kyndryl. Поставщик отдельно проверяет такую архитектуру сети и применяет меры по предотвращению несанкционированных сетевых подключений к системам, приложениям и сетевым устройствам на предмет соответствия стандартам безопасного сегментирования, изоляции и углубленной защиты. Поставщик не имеет права использовать беспроводные технологии при размещении и эксплуатации любых Хост-служб; в остальном Поставщик может использовать беспроводные сетевые технологии при предоставлении Услуг и Конечных продуктов и при обработке Технологии Kyndryl, но Поставщик должен выполнять шифрование и требовать безопасной аутентификации для любых таких беспроводных сетей.

4.2 Поставщик должен поддерживать меры, направленные на логическое разделение и предотвращение демонстрации Материалов Kyndryl неавторизованным лицам или предоставления таким лицам доступа к ним. Кроме того, Поставщик должен поддерживать соответствующую изоляцию своих производственных, непроизводственных и других сред и — если Материалы Kyndryl уже присутствуют в непроизводственной среде или передаются в непроизводственную среду (например, для воспроизведения ошибки) — обеспечить защиту безопасности и конфиденциальности в непроизводственной среде, равную защите в производственной среде.

4.3 Поставщик должен шифровать Материалы Kyndryl при транспортировке и хранении (если только Поставщик не продемонстрирует Kyndryl в разумных пределах, что шифрование Материалов Kyndryl при хранении технически неосуществимо). Поставщик также должен шифровать все физические носители, если таковые имеются, например носители, содержащие файлы резервного копирования. Поставщик поддерживает задокументированные процедуры безопасного генерирования, выдачи, распространения, хранения, ротации, отзыва, восстановления, резервного копирования, уничтожения, доступа и использования ключей, связанных с шифрованием данных. Поставщик гарантирует, что конкретные криптографические методы, используемые для такого шифрования, соответствуют Передовой отраслевой практике (например NIST SP 800-131a).

4.4 Если Поставщику требуется доступ к Материалам Kyndryl, Поставщик ограничит и снизит такой доступ до минимального уровня, необходимого для предоставления и поддержки Услуг и

Конечных продуктов. Поставщик должен требовать, чтобы такой доступ, включая административный доступ к любым базовым компонентам (т. е. привилегированный доступ), был индивидуальным, основанным на ролях и подлежал утверждению и регулярной проверке уполномоченными сотрудниками Поставщика в соответствии с принципами разделения обязанностей. Поставщик должен поддерживать меры по выявлению и удалению избыточных и неактивных учетных записей. Поставщик также аннулирует учетные записи с привилегированным доступом в течение 24 (двадцати четырех) часов после увольнения владельца учетной записи или по требованию Kyndryl или любого уполномоченного сотрудника Поставщика, например руководителя владельца учетной записи.

4.5 В соответствии с Передовой отраслевой практикой Поставщик поддерживает технические меры, обеспечивающие тайм-аут неактивных сессий, блокировку учетных записей после нескольких последовательных неудачных попыток входа, надежную аутентификацию пароля или парольной фразы, а также меры, требующие безопасной передачи и хранения таких паролей и парольных фраз. Кроме того, Поставщик должен использовать многофакторную аутентификацию для всех неконсольных привилегированных доступов к любым Материалам Kyndryl.

4.6 Поставщик должен отслеживать использование привилегированного доступа и поддерживать меры по управлению информацией и событиями безопасности, направленные на: (а) выявление несанкционированного доступа и деятельности, (b) содействие своевременному и надлежащему реагированию на такой доступ и деятельность, и (c) обеспечение возможности проведения аудитов Поставщиком, Kyndryl (в соответствии с ее правами проверки в настоящих Условиях и правами аудита в Документе о транзакции или связанном базовом или другом связанном соглашении между сторонами) и другими лицами в рамках соблюдения документированной политики Поставщика.

4.7 Поставщик хранит журналы, в которых он регистрирует в соответствии с Передовой отраслевой практикой весь административный, пользовательский или иной доступ к системам или деятельность в отношении систем, используемых при предоставлении Услуг или Конечных продуктов и при Взаимодействии с Технологией Kyndryl (и предоставляет эти журналы Kyndryl по запросу). Поставщик принимает меры, направленные на защиту от несанкционированного доступа, модификации, а также случайного или преднамеренного уничтожения таких журналов.

4.8 Поставщик поддерживает компьютерную защиту систем, которыми он владеет или управляет, включая системы конечных пользователей, и которые он использует при предоставлении Услуг или Конечных продуктов или при Взаимодействии с Технологией Kyndryl, причем такая защита включает: брандмауэры конечных точек, полное шифрование диска, технологии обнаружения и реагирования на конечные точки на основе подписи и без подписи для борьбы с вредоносными программами и современными постоянными угрозами, блокировки экрана на основе времени и решения по управлению конечными точками, которые обеспечивают соблюдение конфигурации защиты и требований к исправлениям. Кроме того, Поставщик реализует технические и операционные средства контроля, гарантирующие, что только известным и доверенным системам конечных пользователей разрешено использовать сети Поставщика.

4.9 В соответствии с Передовой отраслевой практикой Поставщик обеспечивает защиту сред центров обработки данных, в которых находятся или обрабатываются материалы Kyndryl, причем такая защита включает в себя обнаружение и предотвращение вторжений, а также меры противодействия атакам типа «отказ в обслуживании» и функции защиты от сбоя.

5. Контроль целостности и доступности Услуг и Систем

5.1 Поставщик обязуется: (а) проводить оценку рисков безопасности и конфиденциальности не реже одного раза в год, (b) проводить тестирование защиты и оценивать уязвимости, включая автоматизированное сканирование безопасности систем и приложений и ручной этический взлом, до выпуска продукции и ежегодно после этого в отношении Услуг и Конечных продуктов, а также ежегодно в отношении Взаимодействия с Технологией Kyndryl, (c) привлекать квалифицированную независимую третью сторону для проведения тестирования на проникновение в соответствии с Передовой отраслевой практикой не реже одного раза в год, причем такое тестирование включает как автоматизированное, так и ручное тестирование, (d) осуществлять автоматизированное управление и обычную проверку соответствия требованиям конфигурации защиты для каждого компонента Услуг и

Конечных продуктов, а также в отношении Взаимодействия с Технологией Kyndryl, и (е) устранять выявленные уязвимости или несоответствия требованиям конфигурации защиты на основе соответствующего риска, возможности использования и воздействия. Поставщик предпринимает разумные шаги, чтобы избежать сбоя Услуг при проведении тестов, оценок, сканирования и при выполнении мероприятий по исправлению. По запросу Kyndryl Поставщик предоставляет Kyndryl письменную сводку последних мероприятий Поставщика по тестированию на проникновение, отчет по которому, как минимум, включает в себя название предложений, охваченных тестированием, количество систем или приложений в области тестирования, даты тестирования, методологию, использованную при тестировании, и детальную сводку результатов.

5.2 Поставщик должен поддерживать политику и процедуры, разработанные для управления рисками, связанными с внесением изменений в Услуги или Конечные продукты или в порядок Взаимодействия с Технологией Kyndryl. Перед внедрением такого изменения, в том числе в затронутые системы, сети и базовые компоненты, Поставщик документирует в зарегистрированном запросе на изменение: (а) описание и причину изменения, (b) детали и график реализации, (c) заявление о рисках, касающееся воздействия на Услуги и Конечные Продукты, заказчиков Услуг или Материалы Kyndryl, (d) ожидаемый результат, (e) план отката и (f) утверждение уполномоченными сотрудниками Поставщика.

5.3 Поставщик ведет инвентарный учет всех ИТ-активов, которые он использует при оказании Услуг, предоставлении Конечных продуктов и Взаимодействии с Технологией Kyndryl. Поставщик постоянно контролирует и управляет состоянием (и в том числе емкостью) и доступностью таких ИТ-активов, Услуг, Конечных продуктов и Технологий Kyndryl, включая базовые компоненты таких активов, Услуг, Конечных продуктов и Технологий Kyndryl.

5.4 Поставщик компонует все системы, которые он использует при разработке или эксплуатации Услуг и Конечных продуктов и при Взаимодействии с Технологией Kyndryl, на основе заранее определенных образов безопасности системы или базовых показателей безопасности, которые соответствуют Передовой отраслевой практике, например контрольным показателям Центра интернет-безопасности (CIS).

5.5 Не ограничивая обязательств Поставщика и прав Kyndryl по Документу о транзакции или связанному базовому соглашению между сторонами в отношении непрерывности бизнеса, Поставщик должен по отдельности оценивать каждую Услугу и Конечный продукт и каждую ИТ-систему, используемую при Взаимодействии с Технологией Kyndryl, на предмет соответствия требованиям непрерывности бизнеса и ИТ и аварийного восстановления в соответствии с документированным руководством по управлению рисками. Поставщик гарантирует, что каждая такая Услуга, Конечный продукт и ИТ-система имеет — в той степени, в которой это оправдано такой оценкой риска, — отдельно определенные, документированные, поддерживаемые и ежегодно проверяемые планы обеспечения непрерывности бизнеса и ИТ и аварийного восстановления в соответствии с Передовой отраслевой практикой. Поставщик гарантирует разработку таких планов для обеспечения конкретных сроков восстановления, которые указаны в Разделе 5.6 ниже.

5.6 Конкретные цели точки восстановления («ЦТВ») и цели времени восстановления («ЦВВ») в отношении любой Хост-службы составляют: 24 часа ЦТВ и 24 часа ЦВВ; тем не менее, Поставщик должен соблюдать любой более короткий срок ЦТВ или ЦВВ, который Kyndryl установил для Заказчика, сразу же после предоставления Kyndryl уведомления Поставщику в письменной форме о таком более коротком сроке ЦТВ или ЦВВ (электронное сообщение представляет собой сообщение в письменной форме). Что касается всех других Услуг, предоставляемых Поставщиком Kyndryl, Поставщик гарантирует, что его планы обеспечения непрерывности бизнеса и аварийного восстановления разработаны для обеспечения ЦТВ или ЦВВ, которые позволяют Поставщику соблюдать все его обязательства перед Kyndryl по Документу о транзакции и связанному базовому соглашению между сторонами, а также настоящим Условием, включая его обязательства по своевременному предоставлению тестирования, поддержки и технического обслуживания.

5.7 Поставщик поддерживает меры, направленные на оценку, тестирование и внесение исправлений, содержащих рекомендации по защите, в Услуги и Конечные Продукты и в связанные

системы, сети, приложения и базовые компоненты в рамках таких Услуг и Конечных продуктов, а также в системы, сети, приложения и базовые компоненты, используемые для Взаимодействия с Технологией Kyndryl. После определения того, что исправление, содержащее рекомендации по защите, применимо и уместно, Поставщик вносит исправление в соответствии с документированными рекомендациями по оценке серьезности и риска. Внедрение Поставщиком исправлений, содержащих рекомендации по защите, осуществляется в соответствии с политикой управления изменениями.

5.8 Если Kyndryl имеет разумные основания полагать, что аппаратное или программное обеспечение, которое Поставщик предоставляет Kyndryl, может содержать элементы вторжения, такие как программы-шпионы, вредоносные программы или вредоносный код, то Поставщик должен своевременно работать совместно с Kyndryl над проведением расследования и устранением проблем Kyndryl.

6. Предоставление Услуг

6.1 Поставщик поддерживает общепринятые в отрасли методы федеративной аутентификации для любых учетных записей пользователей или Заказчиков Kyndryl, при этом Поставщик должен следовать Передовой отраслевой практике в области аутентификации таких учетных записей пользователей или Заказчиков Kyndryl (например, с помощью централизованно управляемого Kyndryl многофакторного единого входа в систему, используя OpenID Connect или SAML).

7. Субподрядчики. Не ограничивая обязательств Поставщика или прав Kyndryl в соответствии с Документом о транзакции или связанным базовым соглашением между сторонами в отношении удержания субподрядчиков, Поставщик гарантирует, что любой субподрядчик, выполняющий работу для Поставщика, внедрил средства контроля управления для соблюдения требований и обязательств, которые возложены на Поставщика в рамках настоящих Условий.

8. Физические носители. Поставщик надежно обезвреживает физические носители, предназначенные для вторичного использования, до такого вторичного использования и уничтожает физические носители, не предназначенные для вторичного использования, в соответствии с Передовой отраслевой практикой по обезвреживанию носителей.

Статья IX. Сертификаты и Отчеты Хост-служб

Настоящая Статья применяется, если Поставщик предоставляет Kyndryl Хост-службу.

1.1 Поставщик должен получить следующие сертификаты или отчеты в сроки, указанные ниже:

Сертификаты / отчеты	Сроки
<p>В отношении Хост-служб Поставщика:</p> <p>Сертификат соответствия стандарту ISO 27001, Информационные технологии, Методы обеспечения безопасности, Системы управления информационной безопасностью, причем такой сертификат основывается на оценке авторитетного независимого аудитора.</p> <p>Или</p> <p>Сертификат соответствия Типа 2: Отчет авторитетного независимого аудитора, демонстрирующий проверку систем, средств контроля и операций поставщика в соответствии с Сертификатом 2 Типа 2 (включая, как минимум, безопасность, конфиденциальность и доступность).</p>	<p>Поставщик получает сертификат ISO 27001 в течение 120 дней с момента вступления в силу Документа о транзакции* или Даты предположения**, а затем продлевает сертификат на основе оценки авторитетного независимого аудитора через каждые 12 месяцев после этого (при каждом продлении на основе самой последней версии стандарта).</p> <p>Поставщик получает отчет по Сертификату соответствия 2 Типа 2 в течение 240 дней после даты вступления в силу Документа о транзакции* или Даты предположения**, а затем получает новый отчет авторитетного независимого аудитора, демонстрирующий проверку систем, средств контроля и операций Поставщика в соответствии с Сертификатом соответствия 2 Типа 2 (включая, как минимум, безопасность, конфиденциальность и доступность) через каждые 12 месяцев после этого.</p> <p>* Если на такую дату вступления в силу Поставщик предоставляет Хост-службу.</p> <p>** Дата, по состоянию на которую Поставщик принимает на себя обязательство по предоставлению Хост-службы.</p>

1.2 Если Поставщик запрашивает в письменной форме, а Kyndryl дает письменное согласие, Поставщик может получить эквивалентный по существу указанным выше сертификат или отчет, при том понимании, что сроки, указанные в таблице выше, будут применяться без изменений в отношении эквивалентного по существу сертификата или отчета.

1.3 Поставщик обязуется: (а) по запросу незамедлительно предоставлять Kyndryl копию каждого сертификата и отчета, которые Поставщик обязан получить, и (b) незамедлительно устранять любые недостатки внутреннего контроля, отмеченные в ходе проверок на получение сертификата соответствия 2 или эквивалентных по существу проверок (по согласованию с Kyndryl).

Статья X. Сотрудничество, Проверка и Исправление

Настоящая Статья применяется в том случае, если Поставщик предоставляет Kyndryl Услуги или Конечные продукты.

1. Сотрудничество с Поставщиком

1.1 Если у Kyndryl есть основания сомневаться в том, что какие-либо Услуги или Конечные продукты могли способствовать, способствуют или будут способствовать возникновению какой-либо проблемы кибербезопасности, то Поставщик должен разумно сотрудничать в рамках любого запроса Kyndryl относительно такой проблемы, включая своевременный и полный ответ на запросы о предоставлении информации, будь то документы, другие записи, интервью с соответствующим Персоналом Поставщика или тому подобное.

1.2 Стороны соглашаются: (а) предоставлять по запросу друг друга такую дополнительную информацию, (б) оформлять и передавать друг другу такие другие документы и (с) совершать такие другие действия и поступки, которые другая сторона может обоснованно потребовать в целях реализации намерений настоящих Условий и документов, упомянутых в настоящих Условиях. Например, по запросу Kyndryl Поставщик своевременно предоставляет условия в области конфиденциальности и безопасности из своих письменных договоров с Подрядчиками Обработчика и субподрядчиками, включая (если Поставщик имеет на это право) предоставление доступа к самим договорам.

1.3 По запросу Kyndryl Поставщик своевременно предоставляет информацию о странах, в которых его Конечные продукты и компоненты этих Конечных продуктов были произведены, разработаны или иным образом получены.

2. Проверка (далее в тексте «Объект» – это физическое место, в котором Поставщик размещает, обрабатывает или иным образом получает доступ к Материалам Kyndryl)

2.1 Поставщик должен вести подлежащий аудиту учетный документ, подтверждающий соответствие требованиям настоящих Условий.

2.2 Kyndryl самостоятельно или с помощью внешнего аудитора может (после предварительного письменного уведомления Поставщика за 30 Дней) проверить соблюдение Поставщиком настоящих Условий, в том числе путем доступа к любому Объекту или Объектам для таких целей, хотя Kyndryl не будет получать доступ к любому центру обработки данных, где Поставщик обрабатывает Данные Kyndryl, если у него нет уважительных оснований полагать, что это позволит получить соответствующую информацию. Поставщик должен сотрудничать с Kyndryl при проведении проверки, в том числе своевременно и в полном объеме отвечать на запросы о предоставлении информации, будь то документы, другие записи, интервью с соответствующим персоналом Поставщика и тому подобное. Поставщик может предложить на рассмотрение Kyndryl доказательства соблюдения утвержденных норм поведения или отраслевого сертификата или иным образом предоставить информацию, подтверждающую соблюдение требований настоящих Условий.

2.3 Проверка должна проводиться не более одного раза за любой 12-месячный период, за исключением следующих случаев: (а) Kyndryl проверяет устранение Поставщиком проблем, возникших в результате предыдущей проверки в течение 12-месячного периода, или (б) произошло Нарушение безопасности, и Kyndryl желает проверить соблюдение обязательств, связанных с нарушением. В любом случае Kyndryl предоставляет письменное уведомление за 30 Дней, как указано в Разделе 2.2 выше, но срочность устранения Нарушения безопасности может потребовать от Kyndryl проведения проверки менее чем за 30 Дней до письменного уведомления.

2.4. Регулятор или другой Оператор персональных данных может осуществлять те же права, что и Kyndryl в Разделах 2.2 и 2.3, при том понимании, что регулятор может осуществлять любые дополнительные права, которыми он обладает в рамках закона.

2.5 Если Kyndryl имеет разумные основания полагать, что Поставщик не соблюдает какие-либо из настоящих Условий (независимо от того, возникает ли такое основание в результате проверки в рамках настоящих Условий или иным образом), Поставщик незамедлительно устраняет такое несоответствие.

3. Программа по борьбе с контрафактной продукцией

3.1 Если Конечные продукты Поставщика включают электронные компоненты (например жесткие диски, твердотельные диски, память, центральные процессоры, логические устройства или кабели), Поставщик должен поддерживать и соблюдать документированную программу по предотвращению контрафакта, чтобы, во-первых, предотвратить предоставление Поставщиком Kyndryl контрафактных компонентов и, во-вторых, быстро обнаружить и устранить любой случай, когда Поставщик по ошибке предоставляет Kyndryl контрафактные компоненты. Поставщик возлагает такое же обязательство по поддержанию и соблюдению документированной программы предотвращения контрафакта на всех своих поставщиков, которые предоставляют электронные компоненты, включенные в Конечные продукты Поставщика для Kyndryl.

4. Исправление

4.1 Если Поставщик не выполняет какое-либо из своих обязательств по настоящим Условиям и это невыполнение приводит к Нарушению безопасности, то Поставщик обязуется исправить невыполнение своих обязательств и устранить вредные последствия Нарушения безопасности, причем такое выполнение и устранение последствий будет осуществляться по разумному указанию компании Kyndryl и в указанные ею разумные сроки. Если, однако, Нарушение безопасности возникает в результате предоставления Поставщиком многопользовательской Хост-службы и, следовательно, затрагивает многих заказчиков Поставщика, включая Kyndryl, Поставщик, учитывая характер Нарушения безопасности, своевременно и надлежащим образом исправляет невыполнение и устраняет вредные последствия Нарушения безопасности, уделяя при этом должное внимание любым входным данным Kyndryl в таких исправлениях и устранениях последствий. Без ущерба для вышеизложенного, Поставщик должен без неоправданной задержки уведомить Kyndryl, если Поставщик больше не может соблюдать обязательства, установленные применимым законом о защите данных.

4.2 Kyndryl имеет право участвовать в устранении любого Нарушения безопасности, упомянутого в Разделе 4.1, если сочтет это уместным или необходимым, а Поставщик несет ответственность за свои расходы и затраты на исправление выполненного и за расходы и затраты на устранение последствий, которые стороны понесут в связи с любым таким Нарушением безопасности.

4.3 В качестве примера, затраты и расходы на устранение последствий, связанные с Нарушением безопасности, могут включать затраты и расходы на обнаружение и расследование Нарушения безопасности, определение ответственности в соответствии с применимыми законами и нормативными актами, предоставление уведомлений о нарушении, создание и обслуживание колл-центров, предоставление услуг кредитного мониторинга и восстановления кредитоспособности, перезагрузку данных, исправление дефектов продукта (в том числе посредством Исходного кода или других разработок), привлечение третьих сторон для оказания помощи в вышеуказанной или другой соответствующей деятельности, а также другие затраты и расходы, необходимые для устранения вредных последствий Нарушения безопасности. Для ясности, затраты и расходы на устранение последствий не включают потерю Kyndryl прибыли, бизнеса, стоимости, дохода, нематериальных активов или ожидаемой экономии.