Статья I, Деловая Контактная Информация

Данная Статья применяется, если Поставщик или Kyndryl обрабатывают ДКИ другой стороны.

1.1 Kyndryl и Поставщик могут Обрабатывать ДКИ другой стороны тогда, когда они ведут коммерческую деятельность в связи с предоставлением Поставщиком Услуг и Поставляемых материалов.

1.2 Сторона:

a) обязуется не использовать и не раскрывать ДКИ другой стороны в любых других целях (во избежание разночтений: каждая из сторон обязуется не Продавать ДКИ другой стороны и не использовать или не раскрывать ДКИ другой стороны в любых маркетинговых целях без предварительного письменного согласия другой стороны, а в случаях, когда это необходимо, также без предварительного письменного согласия всех затрагиваемых Субъектов Персональных Данных), и

b) обязуется удалить, изменить, исправить, вернуть, предоставить информацию об Обработке, ограничить Обработку и выполнить любые другие действия по разумному запросу в отношении ДКИ другой стороны – безотлагательно по письменному требованию другой стороны.

1.3 Стороны не вступают в отношения совместных Операторов применительно к ДКИ другой стороны, и предоставление Документа по Транзакции не может рассматриваться в качестве свидетельства какого бы то ни было намерения вступить в отношения совместных Операторов.

1.4 В Политике конфиденциальности Kyndryl на странице https://www.kyndryl.com/privacy приведены дополнительные сведения об обработке ДКИ компанией Kyndryl.

1.5 Каждая из сторон внедрила и обязуется поддерживать технические и организационные меры безопасности для защиты ДКИ другой стороны от потери, уничтожения, изменения, непреднамеренного и несанкционированного раскрытия, непреднамеренного и несанкционированного доступа и неправомерной Обработки.

1.6 Поставщик обязуется безотлагательно (и при любых обстоятельствах в пределах 48 часов) уведомлять Kyndryl о любых ставших ему известных случаях Нарушений безопасности в отношении ДКИ Kyndryl. Поставщик обязуется предоставить 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 объёме, в котором они имеют отношение к нарушению или к действиям Поставщика по устранению последствий и восстановлению работоспособности.

1.7 Если Поставщик только Обрабатывает ДКИ Kyndryl и не имеет доступа к другим данным и материалам, равно как к любым Корпоративным системам Kyndryl, к такой Обработке применяются только данная Статья и Статья X (Содействие, Проверка и Устранение последствий).

Статья II, Технические и организационные меры, Безопасность данных

Данная Статья применяется, если Поставщик Обрабатывает Данные Kyndryl, отличные от ДКИ Kyndryl. Поставщик обязуется соблюдать требования данной Статьи при предоставлении всех Услуг и Поставляемых материалов и тем самым защищать Данные Kyndryl от потери, уничтожения, изменения, непреднамеренного или несанкционированного раскрытия, непреднамеренного или несанкционированного доступа, равно как неправомерной Обработки. Требования данной Статьи распространяются на все ИТ-приложения, платформы и инфраструктуру, эксплуатируемые или управляемые Поставщиком при предоставлении Поставляемых материалов 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 Kyndryl или прилагать к Данным Kyndryl любую другую информацию или данные, включая Персональные Данные, без предварительного письменного согласия Kyndryl; Поставщик не имеет права пользоваться Данными Kyndryl в любой форме, в том числе в обобщённой форме, в целях, отличных от предоставления Услуг и Поставляемых материалов (например, Поставщик не имеет права использовать и повторно использовать Данные Kyndryl для оценки эффективности или в качестве средства улучшения предложений Поставщика, в целях НИОКР для создания новых предложений, равно как для создания отчётов о предложениях Поставщика). За исключением случаев, когда это прямо разрешено Документом по Транзакции, Поставщику запрещено Продавать Данные Kyndryl.

1.2. Поставщик обязуется не встраивать технологии веб-слежения в Поставляемые материалы и в состав Услуг (примерами таких технологий могут быть HTML5, локальные хранилища, сторонние теги и маркеры, веб-маяки), за исключением случаев, когда это прямо разрешено Документом по Транзакции.

2. Запросы третьих лиц и конфиденциальность

2.1. Поставщик не будет раскрывать Данные Kyndryl каким-либо третьим лицам за исключением тех случаев, когда это заранее разрешено Kyndryl в письменной форме. Если государственный орган, в том числе любой регулирующий орган, потребует доступа к Данным Kyndryl (например, если правительство США издаст в интересах национальной безопасности распоряжение в адрес Поставщика о получении Данных Kyndryl), равно как если раскрытия Данных Kyndryl потребует закон, Поставщик обязуется уведомить Kyndryl в письменном виде о таком требовании и предоставит Kyndryl разумную возможность по подаче возражений против такого раскрытия (в ситуациях, когда закон запрещает такое уведомление, Поставщик обязуется принять меры, которые он сочтёт разумными, по подаче возражений против такого запрета и раскрытия Данных Kyndryl, через судебные или иные механизмы).

2.2. Поставщик гарантирует Kyndryl, что: (a) доступ к Данным Kyndryl будет только у тех сотрудников Поставщика, которым он необходим для предоставления Услуг и Поставляемых материалов и только в объёме, необходимом для предоставления Услуг и Поставляемых материалов; (b) на его сотрудников наложены обязательства по конфиденциальности, требующие от этих сотрудников использования и раскрытия Данных Kyndryl только в соответствии с настоящими Положениями.

3. Возврат и удаление Данных Kyndryl

3.1. Поставщик обязуется, по выбору Kyndryl, удалить или вернуть Данные Kyndryl компании Kyndryl при расторжении или прекращении действия Документа по Транзакции, либо раньше по запросу Kyndryl. Если Kyndryl потребует удаления, Поставщик обязуется, в соответствии с Передовой отраслевой практикой, сделать данные нечитаемыми и невосстановимыми, и подтвердит Kyndryl факт их удаления. Если Kyndryl потребует возврата данных Kyndryl,

Поставщик сделает это в соответствии с разумным графиком Kyndryl и разумными письменными инструкциями Kyndryl.

Статья III, Конфиденциальность

Данная Статья применяется, если Поставщик Обрабатывает Персональные Данные Kyndryl.

1. Обработка

1.1 Kyndryl назначает Поставщика Обработчиком Персональных Данных Kyndryl исключительно в целях предоставления Поставляемых материалов и Услуг в соответствии с инструкциями Kyndryl, включая инструкции, содержащиеся в настоящих Положениях, в Документе по Транзакции и в соответствующем базовом соглашении между сторонами. В случае невыполнения Поставщиком инструкций Kyndryl может прекратить использование затронутой части Услуги, направив письменное уведомление. Если Поставщик считает, что инструкция нарушает закон о защите данных, Поставщик обязан безотлагательно проинформировать об этом Kyndryl в течение установленного законом срока.

1.2 Поставщик будет соблюдать все законы о защите данных, применимые к Услугам и Поставляемым материалам.

1.3 Приложение к Документу по Транзакции или сам Документ по Транзакции описывают следующие понятия, относящиеся к Данным Kyndryl:

(a) категории Субъектов Персональных Данных;
(b) типы Персональных Данных Kyndryl;
(c) действия с данными и процедуры Обработки;
(d) длительность и периодичность Обработки; и
(e) список Подрядчиков обработчиков.

2. Технические и организационные меры

2.1 Поставщик обязуется внедрить и поддерживать технические и организационные меры, предусмотренные Статьёй II (Технические и организационные меры, Безопасность данных) и Статьёй VIII (Технические и организационные меры, Общая безопасность), тем самым обеспечив уровень безопасности, соответствующий риску, исходящему от его Услуг и Поставляемых материалов. Поставщик удостоверяет и понимает ограничения, изложенные в Статье II, настоящей Статье III и Статье VIII, и обязуется соблюдать их.

3. Права и запросы Субъектов Персональных Данных

3.1 Поставщик обязуется безотлагательно информировать Kyndryl (по графику, позволяющему Kyndryl и Другим Операторам выполнять свои обязанности, предусмотренные законом) обо всех запросах Субъектов Персональных Данных по реализации прав Субъектов Персональных Данных (включая исправление, удаление и блокирование данных), касающихся Персональных Данных Kyndryl. Поставщик может также оперативно перенаправлять Субъектов Персональных Данных, осуществляющих такие запросы, в Kyndryl. Поставщик не должен отвечать на какие-либо запросы от Субъектов Персональных Данных, если это не требуется законом или Kyndryl не направила указания об этом в письменной форме.

3.2 Если Kyndryl обязана предоставлять информацию, касающуюся Персональных Данных Kyndryl, Другим Операторам или третьим лицам (например, Субъектам Персональных Данных или регулирующим органам), Поставщик обязуется оказывать Kyndryl содействие в этом путём предоставления информации и принятия других разумных мер по запросу Kyndryl по графику, позволяющему Kyndryl своевременно отвечать таким Другим Операторам и третьим лицам.

4. Подрядчики обработчика

4.1 Поставщик обязуется заблаговременно уведомлять Kyndryl в письменном виде перед добавлением новых Подрядчиков обработчика или расширением объёма Обработки имеющимся Подрядчиком обработчика, причём в таком уведомлении должны содержаться наименование Подрядчика обработчика и описание нового или расширенного объёма Обработки. Kyndryl имеет право выдвинуть разумные возражения против добавления нового Подрядчика обработчика или расширения объёма в любое время, и в этом случае стороны будут совместно добросовестно стремиться урегулировать возражения Kyndryl. С учётом права Kyndryl возразить против этого в любое время Поставщик имеет право привлечь нового Подрядчика обработчика и расширить объём Обработки имеющимся Подрядчиком обработчика в любое время, если Kyndryl не выдвинет возражений в течение 30 Дней с даты подачи Поставщиком письменного уведомления.

4.2 Поставщик установит обязательства по защите данных, безопасности и сертификации, предусмотренные настоящими Положениями, для всех одобренных Подрядчиков обработчика до того, как Подрядчик обработчика начнёт Обрабатывать какие бы то ни было Данные Kyndryl. Поставщик несёт единоличную ответственность перед Kyndryl за выполнение любых обязательств Подрядчиков обработчика.

5. Обработка данных за границей

В нижеследующем тексте:

Страна, обеспечивающая адекватный уровень защиты – страна, в которой обеспечивается адекватный уровень защиты данных в отношении соответствующей передачи данных в соответствии с применимыми законами о защите данных или решениями регулирующих органов.

Импортёр данных – Оператор персональных данных или Подрядчик обработчика, у которого нет представительства в Стране, обеспечивающей адекватный уровень защиты.

Стандартные Договорные Условия ЕС («СДУ ЕС») – Стандартные договорные условия ЕС (Решение Комиссии 2021/914) с дополнительными условиями за исключением пункта 1 Положения 9(a) и пункта 2 Положения 17, официально опубликованные по адресу https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en.

Стандартные Договорные Условия для Сербии («СДУ Сербии») – Стандартные договорные условия Сербии, утверждённые «Комиссаром Сербии по Защите Общественно Значимой Информации и Персональных Данных» и опубликованные по следующему адресу: https://www.poverenik.rs/images/stories/dokumentacija-nova/podzakonski-akti/Klauzulelat.docx.

Стандартные Договорные Условия (**«СДУ»**) – договорные условия, предусмотренные применимыми законами о защите данных в отношении передачи Персональных Данных Операторам, у которых отсутствуют 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 обязуется не передавать и не раскрывать (в том числе путём удаленного доступа) Персональные Данные Kyndryl за рубежом без предварительного письменного согласия Kyndryl. Если Kyndryl даст такое согласие, стороны обязуются совместно обеспечить соблюдение применимого законодательства о защите данных. Если законодательство требует применения СДУ, Поставщик обязуется безотлагательно принять СДУ по требованию Kyndryl.

5.2 В отношении СДУ ЕС:

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

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

(ii) Модуль 2 СДУ ЕС применяется в тех случаях, когда Kyndryl является Оператором Персональных Данных, а модуль 3 применяется, если Kyndryl является Обработчиком Персональных Данных. В соответствии с Положением 13 СДУ ЕС в случае применения Модуля 2 или 3 стороны соглашаются, что (1) СДУ ЕС регулируются законодательством государства-члена ЕС, в котором находится компетентный надзорный орган, и (2) любые споры, возникающие в связи с СДУ ЕС, будут рассматриваться в судах государства-члена ЕС, в котором находится компетентный надзорный орган. Если законодательство из пункта (1) не разрешает права сторонних выгодоприобретателей, то СДУ ЕС будет регулироваться законодательством Нидерландов, и любые споры, возникающие в связи с СДУ ЕС в рамках пункта (2), будут рассматриваться в суде города Амстердама в Нидерландах.

(b) Если Поставщик находится в Европейской Экономической Зоне и Kyndryl является Оператором Персональных Данных, на которого не распространяется Общеевропейский регламент о защите персональных данных 2016/679 (GDPR), то действует Модуль 4 СДУ ЕС и Поставщик заключает СДУ ЕС с Kyndryl в качестве экспортёра данных. Если действует Модуль 4 СДУ ЕС, то стороны соглашаются с тем, что СДУ ЕС будет регулироваться законодательством Нидерландов, и любые споры, возникающие в связи с СДУ ЕС, будут рассматриваться в суде города Амстердама в Нидерландах.

(c) Если Другие Операторы Персональных Данных, такие как Заказчики или аффилированные компании, подадут заявки на присоединение к СДУ ЕС согласно «условию присоединения» Положения 7, то Поставщик настоящим соглашается удовлетворять любые такие заявки.

(d) Технические и организационные меры, необходимые для выполнения требований Приложения II СДУ ЕС, можно найти в настоящих Положениях, в Документе по Транзакции и в соответствующем базовом соглашении между сторонами.

(e) В случае противоречий между СДУ ЕС и данными Положениями преимущественную силу имеют СДУ ЕС.

5.3 В отношении СДУ Соединённого Королевства (СК):

(a) Если у Поставщика отсутствует представительство в Стране, обеспечивающей адекватный уровень защиты: (i) Поставщик заключает СДУ СК с Kyndryl от имени Поставщика как Импортёра данных; и (ii) Поставщик обязуется заключить письменные соглашения со всеми одобренными Подрядчиками обработчика, являющимися Импортёрами данных, в соответствии с Положением 11 СДУ СК, и обязуется предоставить Kyndryl копии таких соглашений по запросу.

(b) Если у Поставщика есть представительство в Стране, обеспечивающей адекватный уровень защиты, Поставщик заключает СДУ СК с Kyndryl от имени всех Подрядчиков обработчика, являющихся Импортёрами данных. Если Поставщик не может сделать этого от имени какого-либо Подрядчика обработчика, Поставщик обязуется предоставить Kyndryl СДУ СК, подписанные этим Подрядчиком обработчика для дальнейшего подписания Kyndryl, прежде чем предоставлять Подрядчику обработчика возможность Обрабатывать любые Персональные Данные Kyndryl.

(c) СДУ СК между Kyndryl и Поставщиком будут выступать в качестве СДУ СК между Оператором персональных данных и Обработчиком или в качестве зеркального письменного соглашения между «импортёром данных» и «подрядчиком обработчика» в соответствии с Положением 11 СДУ СК, в зависимости от фактических обстоятельств. В случае противоречий между СДУ СК и данными Положениями преимущественную силу имеют СДУ СК.

(d) Другие Операторы персональных данных, например Заказчики или аффилированные компании, могут подавать заявки на получение статуса дополнительных «экспортёров данных». Настоящим Поставщик даёт согласие на такие заявки от своего имени и от имени своих Подрядчиков обработчика. Kyndryl обязуется информировать Поставщика обо всех дополнительных «экспортёрах данных»; Поставщик, в свою очередь, обязуется информировать своих Подрядчиков обработчика, являющихся Импортёрами данных, о дополнительных «экспортёрах данных».

5.4 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 Положениями преимущественную силу имеет(-ют) Дополнение(-я) СК.

5.5 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 как Обработчика Персональных Данных; и (ii) Поставщик обязуется заключить письменные соглашения со всеми одобренными Подрядчиками обработчика, являющимися Обработчиками Персональных Данных, в соответствии со Статьёй 8 СДУ Сербии, и обязуется 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, находящихся в Стране, не обеспечивающей адекватный уровень защиты данных. Если Поставщик не может сделать этого от имени какого-либо Подрядчика обработчика, Поставщик обязуется предоставить Kyndryl СДУ Сербии, подписанные этим Подрядчиком обработчика для дальнейшего подписания Kyndryl, прежде чем предоставлять Подрядчику обработчика возможность Обрабатывать любые Персональные Данные Kyndryl.

(c) СДУ Сербии между Kyndryl и Поставщиком будут выступать в качестве СДУ Сербии между Оператором Персональных Данных и Обработчиком Персональных Данных или в качестве зеркального письменного соглашения между «обработчиком» и «подрядчиком обработчика» в зависимости от фактических обстоятельств. В случае противоречий между СДУ Сербии и данными Положениями преимущественную силу имеют СДУ Сербии.

(d) Информация, необходимая для заполнения Приложений 1 – 8 к СДУ Сербии с целью контроля за передачей Персональных Данных в Страну, не обеспечивающую адекватный уровень защиты данных, приводится в настоящих Условиях, в Приложении к Документу по Транзакции или в самом Документе по Транзакции.

5.6 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 Общеевропейский 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. Оказание содействия и ведение учёта

6.1 Принимая во внимание характер Обработки, Поставщик обязуется оказывать Kyndryl содействие в виде принятия надлежащих технических и организационных мер к исполнению обязательств, связанных с запросами и правами Субъектов Персональных Данных. Поставщик

также обязуется оказать Kyndryl содействие в обеспечении выполнения обязательств, связанных с безопасностью Обработки, уведомлением и информированием о Нарушениях безопасности, о проведении оценки влияния на защиту данных, включая предварительные консультации с ответственным регулирующим органом, если это необходимо, принимая во внимание информацию, доступную Поставщику.

6.2 Поставщик обязан вести учёт наименований и контактных сведений каждого Подрядчика обработчика, включая представителя и специалиста по защите данных каждого Подрядчика обработчика. По запросу Поставщик обязуется предоставить учётные документы Kyndryl по графику, позволяющему Kyndryl своевременно ответить на любое требование Заказчика или другого третьего лица.

Статья IV, Технические и организационные меры, Безопасность кода

Данная Статья применяется, если у Поставщика есть доступ к Исходному Коду Kyndryl. Поставщик обязуется соблюдать требования данной Статьи и тем самым защитить Исходный Код Kyndryl от потери, уничтожения, изменения, непреднамеренного или несанкционированного раскрытия, непреднамеренного или несанкционированного доступа, равно как неправомерного Обращения. Требования данной Статьи распространяются на все ИТ-приложения, платформы и инфраструктуру, эксплуатируемые или управляемые Поставщиком при предоставлении Поставляемых материалов и Услуг и Обращении с Технологиями Kyndryl, включая все среды разработки, тестирования, хостинга, поддержки, эксплуатации и центров обработки данных.

1. Требования к безопасности

В нижеследующем тексте:

Запрещённая Страна – любая страна: (a) которую Правительство США назвало иностранным противником в Исполнительном распоряжении от 15 мая 2019 года о защите цепочки поставок информационных и коммуникационных технологий и услуг, (b) включённая в список в соответствии с Разделом 1654 Закона о полномочиях национальной безопасности 2019 года (США), или (c) названная «Запрещённой Страной» в Документе по Транзакции.

1.1. Поставщик обязуется не распространять и не передавать на ответственное хранение Исходный Код Kyndryl в интересах любых третьих лиц.

1.2. Поставщик обязуется не допустить размещения Исходного Кода Kyndryl на серверах, находящихся в Запрещённой Стране. Поставщик обязуется не дать возможности никому, включая его Персонал, находящемуся в Запрещённой Стране или посещающему Запрещённую Страну (на срок такого посещения) по какой бы то ни было причине получить доступ к Исходному Коду Kyndryl или использовать его, вне зависимости от того, где на планете находится Исходный Код; Поставщик не допустит разработки, тестирования и выполнения любых других работ в Запрещённых Странах, если это будет требовать такого доступа или использования.

1.3. Поставщик обязуется не размещать и не распространять Исходный Код Kyndryl в каких бы то ни было юрисдикциях, в которых закон или интерпретация закона требуют раскрытия Исходного Кода третьим лицам. Если в юрисдикции, в которой находится Исходный Код Kyndryl, произойдут изменения в законе или интерпретации закона, требующие раскрытия Исходного Кода третьему лицу, Поставщик обязуется незамедлительно уничтожить или удалить Исходный Код Kyndryl из этой юрисдикции и не размещать другой Исходный Код Kyndryl в этой юрисдикции до тех пор, пока соответствующий закон или интерпретация закона не утратят силу.

1.4. Поставщик обязуется ни прямо, ни косвенно не выполнять никаких действий, включая заключение любых соглашений, которые создадут для Поставщика, Kyndryl или любого третьего лица обязательство по раскрытию информации согласно Разделу 1654 или 1655 Закона о полномочиях национальной безопасности 2019 года (США). Во избежание разночтений: если иное не разрешено прямо в Документе по Транзакции или соответствующем базовом соглашении между сторонами, Поставщик не имеет права раскрывать Исходный Код Kyndryl третьим лицам ни при каких обстоятельствах без предварительного письменного согласия Kyndryl.

1.5. Если Kyndryl уведомит Поставщика или третье лицо уведомит любую из сторон о том, что: (a) Поставщик допустил передачу Исходного Кода Kyndryl в Запрещённую Страну или любую юрисдикцию, указанную в Разделе 1.3 выше, (b) Поставщик иным способом осуществил передачу, доступ или использование Исходного Кода Kyndryl в нарушение Документа по Транзакции или соответствующего базового или иного соглашения между сторонами или (c) Поставщик нарушил положения Раздела 1.4 выше, то без ограничения прав Kyndryl предъявить такое нарушение в соответствии с законодательством, Документом по Транзакции или

соответствующим базовым или иным соглашением между сторонами: (i) если такое уведомление будет подано Поставщику, Поставщик обязуется безотлагательно передать его Kyndryl и (ii) Поставщик в соответствии с разумными указаниями Kyndryl обязуется расследовать сложившуюся ситуацию и ликвидировать её последствия по графику, разумно установленному Kyndryl (после консультаций с Поставщиком).

1.6. Если Kyndryl будет обоснованно полагать, что политики, процедуры, механизмы контроля или практика Поставщика в контексте Исходного Кода будут нуждаться в изменениях для уменьшения рисков в сфере кибербезопасности, хищения интеллектуальной собственности и других аналогичных сферах (включая риск того, что в отсутствие таких изменений Kyndryl может потерять возможность продажи определённым Заказчикам или на определённых рынках или по иным причинам не сможет удовлетворить потребности Заказчиков в сфере безопасности или потребности цепочки поставок), то Kyndryl может связаться с Поставщиком для обсуждения действий, необходимых для уменьшения таких рисков, включая изменение таких политик, процедур, инструментов контроля или практики. По запросу Kyndryl Поставщик обязуется сотрудничать с Kyndryl по вопросам оценки потребности в таких изменениях и внедрения надлежащих согласованных сторонами изменений.

Статья V, Безопасная разработка

Данная Статья применяется в том случае, если Поставщик будет предоставлять Kyndryl принадлежащий ему или третьим лицам Исходный Код или Локальное ПО, а также если Поставляемые материалы или Услуги Поставщика будут предоставляться Заказчику Kyndryl в составе продукта или услуги Kyndryl.

1. Готовность в сфере безопасности

Поставщик обязуется оказывать содействие внутренним процессам Kyndryl, направленным на оценку безопасности продуктов и услуг Kyndryl, зависящих от любых Поставляемых материалов Поставщика, в сфере безопасности, и в том числе своевременно и полно отвечать на запросы информации, будь то в форме документов, других учётных данных, интервью, предоставления Персонала Поставщика и тому подобного.

2. Безопасная разработка

2.1 Данный Раздел 2 применяется только в том случае, если Поставщик предоставляет Локальное ПО компании Kyndryl.

2.2 Поставщик внедрил и обязуется поддерживать на протяжении всего срока действия настоящего Документа по Транзакции, согласно Передовой отраслевой практике, сети, платформы, системы, приложения, устройства, физическую инфраструктуру, средства реагирования на инциденты, а также ориентированные на персонал политики, процедуры и меры обеспечения безопасности, необходимые для защиты: (a) систем и сред разработки, компоновки, тестирования и эксплуатации, которые применяются Поставщиком или любой третьей стороной, привлечённой Поставщиком, в рамках эксплуатации, управления, использования Поставляемых материалов или иных операций по отношению к ним, и (b) исходного кода всех Поставляемых материалов от потери, любых неправомерных форм обработки, а также от несанкционированного доступа, раскрытия или изменения.

3. Сертификация ISO 20243

3.1 Данный Раздел 3 применяется только в том случае, если Поставляемые материалы или Услуги Поставщика будут предоставляться Заказчику Kyndryl в составе продукта или услуги Kyndryl.

3.2 Поставщик обязуется пройти сертификацию на соответствие стандарту ISO 20243, Информационная технология, Открытый стандарт на доверенных поставщиков технологий (O-TTPS), Уменьшение рисков, связанных со злонамеренно испорченной и контрафактной продукцией (либо самостоятельная сертификация, либо сертификация на основе оценки авторитетного независимого аудитора). Как альтернатива, если Поставщик обратится с таким запросом в письменном виде и Kyndryl письменно одобрит этот запрос, Поставщик обязуется пройти сертификацию соответствия эквивалентному по существу отраслевому стандарту, относящемуся к безопасной разработке и цепочкам поставок (в форме самостоятельной сертификации или сертификации на основе оценки авторитетного независимого аудитора, при условии одобрения Kyndryl).

3.3 Поставщик обязуется получить сертификат соответствия стандарту ISO 20243 или эквивалентному по существу отраслевому стандарту (если Kyndryl одобрит это в письменном виде) в течение 180 дней после даты вступления в силу Документа по Транзакции и впоследствии продлевать сертификат каждые 12 месяцев (каждый раз сертификат должен продлеваться для самой последней версии ISO 20243 или, если Kyndryl одобрит это в письменной форме, эквивалентного по существу отраслевого стандарта, относящегося к безопасной разработке и цепочкам поставок).

3.4 Поставщик обязуется по запросу безотлагательно предоставить Kyndryl копию сертификатов, которые Поставщик обязан получить в соответствии с Разделами 2.1 и 2.2 выше.

4. Уязвимости в системе безопасности

В нижеследующем тексте:

Исправление ошибки означает обновления, которые исправляют ошибки или недостатки в Поставляемых материалах, включая Уязвимости в системе безопасности.

Меры по предотвращению негативных последствий означает любые известные средства снижения или предотвращения рисков, связанных с Уязвимостью в системе безопасности.

Уязвимость в системе безопасности означает состояние в проектировании, кодировании, разработке, реализации, тестировании, использовании, поддержке, обслуживании или управлении Поставляемыми материалами, позволяющее стороннему лицу осуществить атаку для несанкционированного доступа или использования системы, включая: (a) просмотр, контроль или нарушение работы системы, (b) просмотр, удаление, изменение или извлечение данных, или (c) изменение профилей, прав доступа или разрешений для пользователей или администраторов. Уязвимость в системе безопасности может существовать независимо от того, присвоен ли ей идентификатор в Общем перечне уязвимостей и рисков (CVE) либо в другой рейтинговой или официальной классификации.

4.1 Поставщик заявляет и гарантирует, что он будет: (a) использовать Передовые отраслевые практики обнаружения Уязвимостей в системе безопасности, включая непрерывное сканирование безопасности приложений со статическим и динамическим анализом исходного кода, сканирование безопасности приложений с открытым исходным кодом, сканирование уязвимостей систем, и (b) обеспечивать соблюдение требований настоящих Положений с целью предотвращения, обнаружения и устранения Уязвимостей в системе безопасности в составе Поставляемых материалов и во всех ИТ-приложениях, платформах и инфраструктурах, задействованных Поставщиком при создании и предоставлении Услуг и Поставляемых материалов.

4.2 Если Поставщику станет известно об Уязвимости в системе безопасности в составе Поставляемых материалов или любых таких ИТ-приложений, платформ или инфраструктур, то Поставщик обязан предоставить Kyndryl Исправление ошибки и Меры по предотвращению негативных последствий для всех версий и выпусков Поставляемых материалов в соответствии с Уровнями серьёзности и временными рамками, указанными в нижеприведённых таблицах:

Уровень серьёзности*
Экстренная уязвимость в системе безопасности – Уязвимость в системе безопасности, представляющая собой серьёзную и потенциально глобальную угрозу. Kyndryl присваивает статус Экстренных уязвимостей в системе безопасности по собственному усмотрению вне зависимости от рейтинга CVSS.
Критический уровень – Уязвимость в системе безопасности с рейтингом от 9 до 10,0 в CVSS.
Высокий уровень – Уязвимость в системе безопасности с рейтингом от 7,0 до 8,9 в CVSS.
Средний уровень – Уязвимость в системе безопасности с рейтингом от 4,0 до 6,9 в CVSS.
Низкий уровень – Уязвимость в системе безопасности с рейтингом от 0,0 до 3,9 в CVSS.

Временные рамки				
Экстренный	***Критический***	***Высокий***	***Средний***	***Низкий***
4 дня или меньше по решению директора по информационной безопасности Kyndryl	30 дней	30 дней	90 дней	Согласно Передовой отраслевой практике

* В любом случае, когда Уязвимости в системе безопасности еще не присвоен рейтинг CVSS, Поставщик будет применять Уровень серьёзности, соответствующий характеру и обстоятельствам такой уязвимости.

4.3 Если Уязвимость в системе безопасности официально обнародована, но Поставщик не предоставил Kyndryl Исправления ошибок или Меры по предотвращению негативных последствий, то Поставщик должен реализовать дополнительные технически осуществимые средства безопасности, позволяющие снизить риски, связанные с уязвимостью.

4.4 Если Kyndryl не удовлетворена реакцией Поставщика на какую-либо Уязвимость в системе безопасности в составе Поставляемых материалов или любого приложения, платформы или инфраструктуры, упомянутых выше, то без ущерба для любых других прав Kyndryl Поставщик должен в кратчайшие сроки организовать для Kyndryl обсуждение данной проблемы непосредственно с Вице-президентом Поставщика или равным по должности руководителем, отвечающим за Исправление ошибок.

4.5 Примеры Уязвимостей в системе безопасности включают код сторонней фирмы или открытый исходный код после прекращения обслуживания (EOS), когда для этих типов кода больше не выпускаются исправления безопасности.

Статья VI, Доступ к Корпоративным системам

Эта Статья применяется, если у сотрудников Поставщика будет доступ к любой Корпоративной системе.

1. Общие положения

1.1 Kyndryl будет решать, предоставлять ли сотрудникам Поставщика разрешение на доступ к Корпоративным системам. Если Kyndryl даст такое разрешение, Поставщик будет соблюдать требования настоящей Статьи и обеспечит их соблюдение своими сотрудниками.

1.2 Kyndryl будет определять способы доступа сотрудников Поставщика к Корпоративным системам, включая возможность доступа таких сотрудников к Корпоративным системам с Устройств Kyndryl или Поставщика.

1.3 Сотрудникам Поставщика будет разрешён доступ к Корпоративным системам, причём только с Устройств, с которых Kyndryl разрешит такой доступ, исключительно для предоставления Услуг. Сотрудники Поставщика не имеют права пользоваться Устройствами, с которых Kyndryl разрешит такой доступ, для оказания услуг любым другим физическим или юридическим лицам, равно как для доступа к любым ИТ-системам, сетям, приложения веб-сайтам, средствам работы с электронной почтой, средствам совместной работы и другим аналогичным системам Поставщика или третьих лиц для оказания Услуг или в связи с ними.

1.4 Во избежание разночтений: сотрудникам Поставщика запрещено пользоваться Устройствами, с которых Kyndryl разрешит доступ к Корпоративным системам, в любых личных целях (например, сотрудникам Поставщика запрещено сохранять свои личные файлы, в том числе музыку, видео, фотографии и другие подобные материалы, на этих Устройствах, а также запрещено пользоваться Интернетом с таких Устройств в личных целях).

1.5 Сотрудникам Поставщика запрещено копировать Материалы Kyndryl, доступные посредством Корпоративной системы, без предварительного письменного разрешения Kyndryl (и ни при каких обстоятельствах не разрешается копировать любые материалы Kyndryl на портативные устройства хранения, такие как диски USB, внешние жёсткие диски и другие подобные предметы).

1.6 По запросу Поставщик обязуется подтвердить с указанием имён сотрудников конкретные Корпоративные системы, к которым его сотрудникам разрешён доступ и к которым они осуществляли доступ, за любой указанный Kyndryl период времени.

1.7 Поставщик обязуется уведомлять Kyndryl в течение двадцати четырёх (24) часов о случаях, когда сотрудник Поставщика с доступом к Корпоративной системе прекращает: (a) трудоустройство у Поставщика или (b) выполнение работ, для которых необходим такой доступ. Поставщик обязуется оказывать содействие Kyndryl по незамедлительному аннулированию доступа для таких бывших или текущих сотрудников.

1.8 Поставщик обязуется незамедлительно сообщать Kyndryl о любых фактических или предполагаемых инцидентах в сфере безопасности (например, о потере Устройств Kyndryl или Поставщика либо несанкционированном доступе к Устройству или данным, материалам или иной информации любого рода) и оказывать Kyndryl содействие в расследовании таких инцидентов.

1.9 Поставщику запрещено разрешать любым агентам, независимым подрядчикам и сотрудникам субподрядчиков доступ к любым Корпоративным системам без предварительного письменного согласия Kyndryl; если Kyndryl даст такое согласие, Поставщик обязуется установить контрактные обязательства для таких лиц и их сотрудников по соблюдению требований данной Статьи, как если бы эти лица были сотрудниками Поставщика, и будет нести перед Kyndryl ответственность за любые действия и бездействие таких лиц и их работодателей в отношении такого доступа к Корпоративным системам.

2. Программное обеспечение устройств

2.1 Поставщик поручит своим сотрудникам своевременно устанавливать всё Программное обеспечение устройств, которое потребуется Kyndryl для организации безопасного доступа к Корпоративным системам. Поставщику и его сотрудникам запрещено создавать помехи для работы такого программного обеспечения и реализуемых им механизмов безопасности.

2.2 Поставщик и его сотрудники обязуются соблюдать Правила настройки устройств, установленные Kyndryl, и сотрудничать с Kyndryl по обеспечению работоспособности программного обеспечения в соответствии с намерениями Kyndryl. В частности, Поставщику запрещено обходить программное блокирование веб-сайтов и автоматическую установку исправлений.

2.3 Сотрудникам Поставщика запрещено использовать Устройства, которыми они пользуются для доступа к Корпоративным системам, равно как их имена пользователей и пароли для доступа к Устройствам и другую аналогичную информацию совместно с любыми другими лицами.

2.4 Если Kyndryl разрешит сотрудникам Поставщика доступ к Корпоративным системам с Устройств Поставщика, Поставщик обязуется установить и выполнять на этих Устройствах разрешённую Kyndryl операционную систему и устанавливать новые версии этой операционной системы или новую операционную систему в разумное время после получения соответствующих инструкций Kyndryl.

3. Надзор и содействие

3.1 Kyndryl имеет безусловное право осуществлять мониторинг и реагирование на потенциальные угрозы вторжения и другие угрозы в сфере кибербезопасности любыми возможными способами из любых точек и с применением любых средств, которые Kyndryl сочтёт необходимыми или надлежащими, без предварительного уведомления Поставщика, сотрудников Поставщика и иных лиц. Например, в рамках данного права Kyndryl может в любое время (a) провести тест безопасности на любом Устройстве, (b) осуществлять мониторинг, восстановление с помощью технических и иных средств и перлюстрацию коммуникаций (включая электронную почту с любых адресов электронной почты), учётных данных, файлов и других элементов, хранящихся на любых Устройствах и передаваемых через любые Корпоративные системы, и (c) получать полные образы любых Устройств, сделанные в интересах безопасности. Если Kyndryl потребуется содействие Поставщика в реализации своих прав, Поставщик обязуется полностью и своевременно выполнять запросы Kyndryl по оказанию такого содействия (включая, например, запросы на безопасную настройку любого Устройства, установку средств мониторинга или другого программного обеспечения на любое Устройство, передачу сведений о соединениях на системном уровне, участие в принятии мер реагирования на инциденты на любом Устройстве и предоставление Kyndryl физического доступа к любому Устройству для получения полного образа в интересах безопасности и в других целях, а также другие аналогичные и связанные с этим 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, любых сотрудников Поставщика и прочих лиц, если Kyndryl будет полагать, что это необходимо для защиты Kyndryl.

3.3 Права Kyndryl не могут быть блокированы, уменьшены или ограничены в любой форме какими бы то ни было положениями Документа по Транзакции, связанного базового соглашения между сторонами или любого другого соглашения между сторонами, включая любые положения, требующие размещения данных, материалов и другой информации любого рода только в определённом месте (или определённых местах) или требующие, чтобы доступ к таким данным, материалам и иной информации осуществлялся только лицами, находящимися в определённом месте (или определённых местах).

4. Устройства Kyndryl

4.1 Kyndryl сохраняет право собственности на все Устройства Kyndryl, причем Поставщик берёт на себя риск потери Устройств, в том числе вследствие хищения, вандализма или халатности. Поставщик не будет вносить и допускать внесение любых изменений в Устройства Kyndryl без предварительного письменного согласия Kyndryl, при этом изменением считается любое изменение Устройства, включая любое изменение программного обеспечения, приложений, элементов безопасности, конфигурации безопасности, физической, механической или электрической конструкции Устройства.

4.2 Поставщик обязуется вернуть все Устройства Kyndryl в течение 5 рабочих дней с момента, когда прекратится потребность в этих Устройствах для оказания Услуг, и по запросу Kyndryl одновременно с этим уничтожить все данные, материалы и прочую информацию любого рода на этих Устройствах, не сохраняя копий и следуя Передовой отраслевой практике по уничтожению таких данных, материалов и прочей информации. Поставщик обязуется упаковать и вернуть Устройства Kyndryl в том же состоянии, в котором они были доставлены Поставщику, за исключением разумного естественного износа, за свой счёт по адресу, указанному Kyndryl. Невыполнение Поставщиком любых обязательств, предусмотренных Разделом 4.2, представляет собой существенное нарушение условий Документа по Транзакции и соответствующего базового соглашения и всех других связанных соглашений между сторонами, с пониманием того, что соглашение считается «связанным», если доступ к любой Корпоративной системе обеспечивает возможность выполнения Поставщиком задач и других работ по этому соглашению.

4.3 Kyndryl будет предоставлять поддержку по Устройствам Kyndryl (включая осмотр Устройств, профилактическое обслуживание и ремонт). Поставщик обязуется безотлагательно сообщать Kyndryl о потребности в ремонте.

4.4 В отношении программ, которые принадлежат или лицензируются Kyndryl, Kyndryl предоставляет Поставщику временное право использовать, хранить и делать достаточное количество копий для поддержки разрешённого использования Устройств Kyndryl. Поставщик не имеет права передавать программы кому бы то ни было, копировать информацию о лицензиях, а также дизассемблировать, декомпилировать, осуществлять обратное проектирование или иным способом преобразовывать любые программы, кроме случаев, когда это прямо разрешено применимым законом без возможности ограничения этих действий в договорном порядке.

5. Обновление

5.1 Безотносительно любых противоречащих этому положений в Документе по Транзакции или в другом базовом соглашении между сторонами, по письменному уведомлению Поставщика и без необходимости получать согласие Поставщика, Kyndryl имеет право обновлять, дополнять и другими способами изменять настоящую Статью для выполнения любых требований, предусмотренных применимым законом или обязательств перед Заказчиками, для отражения любого развития передовой практики в сфере безопасности, а также в других случаях, если Kyndryl посчитает, что это необходимо для защиты Корпоративных систем или Kyndryl.

Статья VII, Дополнение персонала

Данная Статья применяется в случаях, когда сотрудники Поставщика посвящают всё свое рабочее время предоставлению Услуг компании Kyndryl, оказывая эти услуги в помещениях Kyndryl, помещениях Заказчика или из своего дома, пользуясь исключительно Устройствами Kyndryl для доступа к Корпоративным системам.

1. Доступ к Корпоративным системам; среды Kyndryl

1.1 Поставщик имеет право оказывать Услуги только путём доступа к Корпоративным системам с помощью Устройств, предоставленных компанией Kyndryl.

1.2 Поставщик обязуется соблюдать положения Статьи VI (Доступ к Корпоративным системам) в отношении любого доступа к Корпоративным системам.

1.3 Предоставленные компанией Kyndryl устройства представляют собой единственные устройства, которыми Поставщик и его сотрудники могут пользоваться для предоставления Услуг, причём они могут использоваться исключительно Поставщиком и его сотрудниками и только для предоставления Услуг. Во избежание разночтений, ни при каких обстоятельствах Поставщику и его сотрудникам не разрешается пользоваться другими устройствами для оказания Услуг, равно как пользоваться Устройствами Kyndryl в интересах любых других заказчиков Поставщика или в любых целях, отличных от предоставления Услуг компании Kyndryl.

1.4 Сотрудники Поставщика, пользующиеся Устройствами Kyndryl, могут передавать Материалы Kyndryl друг другу и сохранять такие материалы на Устройствах Kyndryl, однако только в ограниченном объёме, в котором такие передача и хранение необходимы для оказания Услуг.

1.5 За исключением такого хранения на Устройствах Kyndryl, Поставщику и его сотрудникам ни при каких обстоятельствах не разрешается удалять любые Материалы Kyndryl из репозиториев, сред, инструментов и инфраструктуры Kyndryl, где они хранятся компанией Kyndryl.

1.6 Во избежание разночтений: Поставщику и его сотрудникам запрещается перемещать любые Материалы Kyndryl в любые репозитории, среды, инструменты или инфраструктуру Поставщика, равно как в любые другие системы, платформы, сети Поставщика и тому подобное, без предварительного письменного согласия Kyndryl.

1.7 Статья VIII (Технические и организационные меры, Общая безопасность) не распространяется на Услуги Поставщика в ситуациях, когда сотрудники Поставщика посвящают всё свое рабочее время предоставлению Услуг компании Kyndryl, оказывая эти Услуги в помещениях Kyndryl, помещениях Заказчика или из своего дома, пользуясь исключительно Устройствами Kyndryl для доступа к Корпоративным системам. В иных случаях Статья VIII применяется к Услугам Поставщика.

Статья VIII, Технические и организационные меры, Общая безопасность

Данная Статья применяется в случаях, когда Поставщик предоставляет любые Услуги или Поставляемые материалы компании Kyndryl, за исключением ситуаций, когда у Поставщика при предоставлении таких Услуг и Поставляемых материалов есть доступ только к ДКИ Kyndryl (то есть, Поставщик не будет Обрабатывать никакие другие Данные Kyndryl и не будет располагать доступом к другим Материалам Kyndryl или Корпоративным системам), Услуги и Поставляемые материалы Поставщика ограничиваются только предоставлением Kyndryl Локального ПО или Поставщик предоставляет все Услуги и Поставляемые материалы по модели дополнения персонала, на которую распространяется Статья VII, включая её Раздел 1.7.

Поставщик обязуется соблюдать требования данной Статьи и тем самым защитить: (a) Материалы Kyndryl от потери, уничтожения, изменения, непреднамеренного или несанкционированного раскрытия, непреднамеренного или несанкционированного доступа, (b) Данные Kyndryl от неправомерной Обработки и (c) Технологии Kyndryl от неправомерного Обращения. Требования данной Статьи распространяются на все ИТ-приложения, платформы и инфраструктуру, эксплуатируемые или управляемые Поставщиком при предоставлении Поставляемых материалов и Услуг и Обращении с Технологиями Kyndryl, включая все среды разработки, тестирования, хостинга, поддержки, эксплуатации и центров обработки данных.

1. Правила безопасности

1.1. Поставщик будет поддерживать и соблюдать политики и практические методы обеспечения ИТ-безопасности, которые являются неотъемлемой частью деятельности Поставщика, обеспечивая их обязательное выполнение всем Персоналом Поставщика в соответствии с Передовыми отраслевыми практиками.

1.2. Поставщик будет пересматривать свою политику и методы обеспечения ИТ-безопасности как минимум раз в год и вносить в них дополнения и правки, необходимые, по мнению Поставщика, для защиты Материалов Kyndryl.

1.3. Поставщик будет соблюдать и выполнять стандартные обязательные требования в отношении проверки данных при трудоустройстве всех новых сотрудников и распространять действие таких требований на весь Персонал Поставщика и все находящиеся в полной собственности Поставщика дочерние компании. Эти требования должны включать проверку на наличие судимостей, в том объёме, в котором это разрешено местным законодательством, проверку подлинности удостоверения личности и дополнительные проверки по усмотрению Поставщика. Поставщик должен периодически повторять и пересматривать требования, которые он сочтёт необходимыми.

1.4. Поставщик должен ежегодно проводить для своих работников обучение в области безопасности и защиты данных и требовать, чтобы все такие работники каждый год подтверждали, что будут соблюдать правила этичного делового поведения Поставщика, политики конфиденциальности и безопасности, установленные в правилах поведения Поставщика или в аналогичных документах. Поставщик обязуется предоставить сотрудникам с административным доступом к любым компонентам Услуг, Поставляемых материалов или Материалов Kyndryl дополнительное обучение, касающееся политики и процессов, которое соответствует роли этих лиц в оказании и поддержке Услуг, Поставляемых материалов и Материалов Kyndryl, насколько это необходимо для поддержания соответствия требованиям и сохранения сертификатов.

1.5. Поставщик обязуется разработать меры обеспечения безопасности и конфиденциальности для защиты и обеспечения доступности Материалов Kyndryl, включая реализацию, обслуживание и соблюдение политик и процедур со встроенными средствами обеспечения безопасности и конфиденциальности, защищённое проектирование и защищённые операции, для всех Услуг и Поставляемых материалов, а также для всех видов Обращения с Технологиями Kyndryl.

2. Нарушения Безопасности

2.1. Поставщик будет поддерживать и соблюдать документально оформленную политику реагирования на нарушения безопасности, соответствующую Передовым отраслевым практикам в отношении нарушений компьютерной безопасности.

2.2. Поставщик должен расследовать неавторизованный доступ или несанкционированное использование Материалов Kyndryl, а также разработать и исполнять соответствующий план реагирования.

2.3. Поставщик обязуется безотлагательно (и при любых обстоятельствах в пределах 48 часов) уведомлять Kyndryl о любых ставших ему известных случаях Нарушений безопасности. Поставщик обязуется предоставить 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 объёме, в котором они имеют отношение к нарушению или к действиям Поставщика по устранению последствий и восстановлению работоспособности.

2.4. Поставщик обязан оказать Kyndryl разумное содействие в выполнении обязательств Kyndryl, аффилированных компаний Kyndryl и Заказчиков (а также их аффилированных компаний и заказчиков), установленных законом (включая обязательства по уведомлению регулирующих органов или Субъектов Персональных Данных), в отношении Нарушения безопасности.

2.5. Поставщик обязуется не информировать и не уведомлять каких бы то ни было третьих лиц о том, что Нарушение безопасности прямо или косвенно связано с Kyndryl или с Материалами Kyndryl, без письменного разрешения Kyndryl или необходимости соблюдения законодательных требований. Поставщик обязан предоставлять Kyndryl письменное уведомление перед распространением уведомлений, требуемых в соответствии с законодательством, любым третьим лицам, если такое уведомление может прямым или косвенным образом привести к идентификации Kyndryl.

2.6. В случае Нарушения безопасности, вызванного нарушением Поставщиком любых обязательств, предусмотренных настоящими Положениями:

(a) Поставщик несёт ответственность по оплате всех своих расходов, а также фактических расходов Kyndryl по направлению уведомлений о Нарушениях безопасности в регулирующие органы, органы государственной власти, отраслевые органы саморегулирования, средства массовой информации (если такая обязанность предусмотрена законом), Субъектам Персональных Данных, Заказчикам и прочим лицам,

(b) по запросу Kyndryl Поставщик обязуется создать и содержать за счёт Поставщика контактный центр, предназначенный для предоставления ответов на вопросы Субъектов Персональных Данных о Нарушении безопасности и его последствиях в течение 1 года с даты уведомления Субъектов Персональных Данных о Нарушении безопасности или в соответствии с требованиями применимого закона о защите данных, в зависимости от того, что предоставляет более обширную защиту. Kyndryl и Поставщик обязуются совместно работать над созданием сценариев и других материалов, которые будут использоваться работниками контактного центра для предоставления ответов на запросы. Возможен также другой вариант, при котором Kyndryl, письменно уведомив Поставщика, может создать и содержать свой контактный центр вместо Поставщика; в этом случае Поставщик обязуется возместить Kyndryl фактические расходы, понесённые Kyndryl в связи с созданием и обслуживанием такого контактного центра, и

(c) Поставщик обязуется возместить Kyndryl фактические расходы, понесённые Kyndryl в связи с предоставлением услуг кредитного мониторинга и восстановления кредитной истории в течение 1 года с даты уведомления лиц, затронутых нарушением безопасности и зарегистрировавшихся для получения таких услуг, о Нарушении безопасности, или в соответствии с требованиями применимого закона о защите данных, в зависимости от того, что предоставляет более обширную защиту.

3. Физическая безопасность и контроль входа (в нижеследующем тексте «Объект» означает физическое место, в котором Поставщик размещает и обрабатывает Материалы Kyndryl и осуществляет доступ к ним).

3.1. Поставщик будет применять надлежащие меры контроля физического входа, например, заграждения, пункты входа с доступом по карточкам, камеры слежения и службы регистрации посетителей, для защиты от несанкционированного проникновения на Объекты.

3.2. Поставщик должен требовать разрешения авторизованных лиц на доступ на Объекты и в контролируемые зоны на своих Объектах, включая временный доступ, и ограничивать доступ в зависимости от должности и служебной необходимости. Любой посетитель, которому Поставщик предоставляет временный доступ, должен находиться на Объекте или в контролируемых зонах только в сопровождении авторизованного сотрудника.

3.3. Поставщик должен внедрить физический контроль доступа, включая многофакторные средства контроля, в соответствии с Передовыми отраслевыми практиками, чтобы надлежащим образом ограничивать доступ в контролируемые зоны в пределах Объектов, а также должен вести журналы всех попыток входа и хранить такие журналы по крайней мере в течение одного года.

3.4. Поставщик должен аннулировать доступ на Объекты и в контролируемые зоны в пределах Объектов (a) после увольнения авторизованного сотрудника Поставщика или b) после того, как у авторизованного сотрудника Поставщика исчезнет обоснованная необходимость для доступа. Поставщик должен следовать документально оформленным процедурам увольнения, которые включают немедленное удаление увольняемых из контрольных списков доступа и возврат электронных пропусков.

3.5. Поставщик должен принимать предупредительные меры для защиты всей физической инфраструктуры, используемой для поддержки Услуг и Поставляемых материалов и для Обращения с Технологиями Kyndryl, от угроз окружающей среды, имеющих как естественную, так и антропогенную природу, таких как аномально высокая температура окружающей среды, пожар, наводнение, повышенная влажность, кража и вандализм.

4. Контроль за доступом, вмешательством, передачей и разделением обязанностей

4.1. Поставщик будет поддерживать документально подтверждённую архитектуру безопасности сетей, которыми Поставщик управляет в процессе работы над Услугами, предоставления Поставляемых материалов и Обращения с Технологиями Kyndryl. Поставщик должен независимо проверять такую архитектуру сетей и предпринимать меры, направленные на предотвращение несанкционированных сетевых соединений с системами, приложениями и сетевыми устройствами, для обеспечения соответствия стандартам безопасной сегментации, изоляции и многоуровневой защиты. Поставщику запрещено использовать беспроводные технологии в связи с хостингом и предоставлением любых Размещённых Услуг; однако Поставщик имеет право использовать беспроводные сетевые технологии в процессе предоставления Услуг и Поставляемых материалов и Обращения с Технологиями Kyndryl, обеспечив шифрование и безопасную идентификацию для любых беспроводных сетей.

4.2. Поставщик должен использовать меры, которые предназначены для логического разграничения и предотвращения воздействия или доступа к Материалам Kyndryl со стороны неавторизованных лиц. Более того, Поставщик должен надлежащим образом изолировать свои производственные, непроизводственные и другие среды и в случае, если Материалы Kyndryl уже присутствуют в непроизводственной среде или передаются в непроизводственную среду (например, с целью воспроизведения ошибки), Поставщик должен реализовать в непроизводственной среде меры обеспечения безопасности и защиты данных, эквивалентные мерам, принятым в производственной среде.

4.3. Поставщик должен обеспечить шифрование хранимых и передаваемых Материалов Kyndryl (если Поставщик не сможет предоставить Kyndryl разумное доказательство того, что шифрование хранимых Материалов Kyndryl технически неосуществимо). Кроме того, Поставщик должен обеспечить шифрование всех физических носителей, если они применяются, таких как носители с резервными копиями файлов. Поставщик будет соблюдать документально зафиксированные процедуры безопасного генерирования, публикации, распространения, хранения, оборота, отзыва, восстановления, резервного копирования, уничтожения, доступа и использования ключей в связи с шифрованием данных. Поставщик должен использовать криптографические методы, соответствующие Передовым отраслевым практикам (таким как NIST SP 800-131a).

4.4. Если Поставщику требуется доступ к Материалам Kyndryl, Поставщик должен ограничивать такой доступ минимальным уровнем, необходимым для предоставления и поддержки Услуг и Поставляемых Материалов. Поставщик должен требовать, чтобы такой доступ, в том числе доступ с правами администратора (привилегированный доступ) к любым лежащим в основе компонентам, предоставлялся на индивидуальной основе, в зависимости от функциональных обязанностей и подлежал утверждению и регулярному пересмотру со стороны авторизованных сотрудников Поставщика с соблюдением принципов разделения обязанностей. Поставщик обязуется принимать меры к выявлению и удалению избыточных и неиспользуемых учётных записей. Поставщик также будет удалять учётные записи с привилегированным доступом в течение двадцати четырёх (24) часов с момента увольнения владельца учётной записи или по запросу Kyndryl или любого уполномоченного сотрудника Поставщика, например руководителя владельца учётной записи.

4.5. В соответствии с Передовыми отраслевыми практиками Поставщик применяет технические методы, обеспечивающие закрытие неактивных сеансов, блокировку учётных записей после нескольких последовательных неудачных попыток входа в систему, использование для аутентификации надёжных паролей или фраз-паролей, а также обеспечивает меры, требующие безопасной передачи и хранения таких паролей и фраз-паролей. Кроме того, Поставщик должен использовать многофакторную аутентификацию для привилегированного доступа к Материалам Kyndryl без применения консоли.

4.6. Поставщик осуществляет контроль за привилегированным доступом и использует информацию о безопасности, а также меры по управлению событиями, предназначенные для (a) обнаружения несанкционированного доступа и действий, (b) упрощения своевременного и надлежащего реагирования на такой доступ и действия и 3) проведения аудита Поставщиком, Kyndryl (в соответствии с правами на проверку, установленными настоящими Положениями, и правами на аудит, указанными в Документе по Транзакции или в соответствующем базовом или ином связанном соглашении между сторонами) и третьими лицами для проверки соблюдения документально оформленной политики Поставщика.

4.7. Поставщик, в соответствии с Передовыми отраслевыми практиками, должен обеспечить хранение журналов с информацией обо всех случаях доступа к системам, используемым для оказания Услуг или предоставления Поставляемых материалов и операциях над ними, а также при Обращении с Технологиями Kyndryl, включая административный доступ и доступ пользователей (и должен предоставлять эти протоколы по запросу Kyndryl). Поставщик применяет меры, предназначенные для защиты от несанкционированного доступа, изменения и случайного или преднамеренного уничтожения таких журналов.

4.8. Поставщик должен применять защиту вычислительных систем, которыми Поставщик владеет или управляет, включая системы конечных пользователей, и которые Поставщик использует для оказания Услуг или предоставления Поставляемых материалов либо при Обращении с Технологиями Kyndryl, включая: брандмауэры на конечных точках, полное шифрование дисков, технологии обнаружения и удаления вредоносного ПО и сложных целенаправленных угроз на основании сигнатур и других методов на конечных точках, блокировку экрана с контролем по времени и решения по управлению конечными устройствами, которые обеспечивают исполнение требования в отношении конфигурации системы безопасности и установки исправлений. Кроме того, Поставщик должен внедрить технические и операционные средства, разрешающие только известным и доверенным системам конечных пользователей использовать сети Поставщика.

4.9. В соответствии с Передовыми отраслевыми практиками Поставщик должен обеспечить защиту центров обработки данных, в которых присутствуют или обрабатываются Материалы Kyndryl, с помощью таких средств обеспечения безопасности, как обнаружение и предотвращение вторжений, а также упреждающие меры по предотвращению и снижению негативных последствий атак с целью отказа в обслуживании.

5. Контроль за целостностью и доступностью Услуги и систем

5.1. Поставщик будет: (a) проводить оценку рисков, связанных с безопасностью и конфиденциальностью, как минимум раз в год, (b) проводить тестирование системы

безопасности и оценку уязвимостей, в том числе автоматизированную проверку безопасности систем и приложений и "этичный взлом" в ручном режиме перед запуском в производство и ежегодно после этого в отношении Услуг и Поставляемых материалов, а также ежегодно в отношении Обращения с Технологиями Kyndryl, (c) привлекать независимых уполномоченных третьих лиц для проведения как минимум раз в год тестирования на возможность проникновения в соответствии с Передовыми отраслевыми практиками, (d) осуществлять автоматизированное управление и стандартную проверку соответствия требованиям к конфигурации системы безопасности для каждого компонента Услуг и Поставляемых материалов, а также в отношении Обращения с Технологиями Kyndryl и (e) устранять выявленные уязвимости или несоответствие требованиям к конфигурации системы безопасности с учётом связанного риска, возможности эксплуатации и воздействия. При проведении тестирования, оценки, проверок и действий по устранению последствий Поставщик будет предпринимать разумные шаги для предотвращения перерывов в работе Услуг. По запросу Kyndryl Поставщик должен предоставлять Kyndryl письменный обзор последних операций по тестированию на возможность проникновения, который должен включать по крайней мере перечень предложений, охваченных тестированием, количество протестированных систем или приложений, даты проведения тестирования, методологию тестирования и общее описание результатов.

5.2. Поставщик будет соблюдать правила и процедуры, предназначенные для управления рисками, связанными с внесением изменений в Услуги или Поставляемые материалы либо с Обращением с Технологиями Kyndryl. Перед реализацией таких изменений в отношении затрагиваемых систем, сетевой инфраструктуры и составляющих компонентов Поставщик должен в документации к зарегистрированному запросу на изменение привести (a) описание и причину изменения, (b) подробные сведения и график реализации, (c) предупреждение о рисках с указанием воздействия на Услуги и Поставляемые материалы, заказчиков Услуг или на Материалы Kyndryl, (d) ожидаемые результаты, (e) план возврата к предыдущему состоянию и (f) одобрение со стороны авторизованных сотрудников Поставщика.

5.3. Поставщик будет вести инвентарный перечень всех ИТ-активов, которые Поставщик использует при оказании Услуг, предоставлении Поставляемых материалов и при Обращении с Технологиями Kyndryl. Поставщик должен непрерывно осуществлять мониторинг и управление работоспособностью (в том числе мощностью) и доступностью таких ИТ-активов, Услуг, Поставляемых материалов и Технологий Kyndryl, включая составляющие компоненты таких активов, Услуг, Поставляемых материалов и Технологий Kyndryl.

5.4. Поставщик должен создавать все системы, применяемые для разработки или предоставления Услуг и Поставляемых материалов и при Обращении с Технологиями Kyndryl, на основе стандартных образов защиты систем или базовых конфигураций безопасности, соответствующих Передовым отраслевым практикам, таким как тесты Center for Internet Security (CIS).

5.5. Без ограничения обязательств Поставщика или прав Kyndryl на основании Документа по Транзакции или связанного базового соглашения между сторонами в отношении непрерывности работы бизнеса, Поставщик должен проводить отдельную оценку каждой Услуги и каждого Поставляемого материала, а также каждой ИТ-системы, используемой при Обращении с Технологиями Kyndryl, на соответствие требованиям к обеспечению непрерывности работы бизнеса и ИТ-инфраструктуры и восстановлению после аварий в соответствии с документально оформленными инструкциями по управлению рисками. Для каждой Услуги, Поставляемого материала и ИТ-системы в той мере, в какой это оправдывается такой оценкой риска, Поставщик должен обеспечивать наличие отдельно разрабатываемых, документируемых, поддерживаемых и ежегодно пересматриваемых планов обеспечения непрерывности работы бизнеса и ИТ-инфраструктуры и восстановления после аварий, согласующихся с Передовыми отраслевыми практиками. Поставщик должен обеспечить разработку таких планов с учётом определённого времени восстановления, указанного ниже в Разделе 5.6.

5.6. Для всех Размещённых Услуг устанавливаются следующие целевые точки восстановления ("**RPO**") и целевое время восстановления ("**RTO**"): 24 часа RPO и 24 часа RTO; при этом Поставщик обязуется обеспечить выполнение более коротких RPO и RTO, которые Kyndryl гарантирует Заказчику, незамедлительно после того, как Kyndryl уведомит Поставщика в письменной форме о подобных изменениях RPO или RTO (сообщение электронной почты считается письменным уведомлением). В той мере, в которой это относится ко всем другим Услугам, предоставляемым Поставщиком Kyndryl, Поставщик должен разработать планы непрерывности деловых операций и аварийного восстановления с учётом RPO и RTO, которые позволят Поставщику соблюдать все его обязательства перед Kyndryl на основании Документа по Транзакции и связанного базового соглашения между сторонами, а также настоящих Положений, включая обязательства по своевременному тестированию, поддержке и обслуживанию.

5.7. Поставщик должен принять меры для оценки, тестирования и применения исправлений, связанных с безопасностью, к Услугам и Поставляемым материалам и к связанным системам, сетевой инфраструктуре, приложениям и компонентам в составе Услуг и Поставляемых материалов, а также к системам, сетевой инфраструктуре, приложениям и компонентам, используемым для Обращения с Технологиями Kyndryl. После того как будет определено, что исправление, связанное с безопасностью, применимо и уместно, Поставщик внедрит исправление в соответствии с документально подтверждённым уровнем серьёзности и инструкциями по оценке рисков. Применение Поставщиком исправлений, связанных с безопасностью, регулируется политикой Поставщика по управлению изменениями.

5.8. Если у Kyndryl будут разумные основания полагать, что аппаратное или программное обеспечение, предоставляемое Поставщиком компании Kyndryl, может содержать элементы неправомерного проникновения, например программы-шпионы, вредоносное программное обеспечение или вредоносный код, Поставщик обязуется оперативно оказать содействие Kyndryl в расследовании предположений Kyndryl и принятии мер реагирования по ним.

6. Предоставление Услуги

6.1 Поставщик должен обеспечить поддержку общепринятых отраслевых методов объединённой аутентификации для любых учётных записей пользователей Kyndryl или Заказчика. Поставщик должен идентифицировать такие учётные записи пользователей Kyndryl или Заказчика с применением Передовых отраслевых практик (таких, как среда единого входа в систему (SSO) с многофакторной идентификацией, централизованно управляемая Kyndryl, с использованием OpenID Connect (OIDC) или Security Assertion Markup Language (SAML).

7. Субподрядчики. Без ограничения обязательств Поставщика или прав Kyndryl на основании Документа по Транзакции или связанного базового соглашения между сторонами в отношении привлечения субподрядчиков, Поставщик обязуется обеспечивать реализацию всеми субподрядчиками, выполняющими работы в интересах Поставщика, мер организационного контроля для соблюдения требований и обязательств, устанавливаемых настоящими Положениями для Поставщика.

8. Физические носители. Поставщик будет безопасным образом удалять не подлежащую распространению информацию с физических носителей, предназначенных для повторного использования, перед таким использованием, и будет уничтожать физические носители, не предназначенные для повторного использования, следуя Передовым отраслевым практикам по очистке носителей данных.

Статья IX, Сертификаты и отчётность по Размещённым Услугам

Данная Статья применяется, если Поставщик предоставляет Kyndryl Размещённую Услугу.

1.1 Поставщик обязуется получить следующие сертификаты или отчёты в соответствии с оговорёнными ниже временными рамками:

Сертификаты/отчеты	**Период времени**
По отношению к предоставлению Поставщиком Размещённых Услуг: Сертификат соответствия «ISO 27001 – Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности» на основе оценки авторитетного независимого аудитора. **или** SOC 2 Типа 2: Отчёт авторитетного независимого аудитора, отражающий результаты проверки систем, средств управления и операций Поставщика в соответствии с SOC 2 Типа 2 (включая, по меньшей мере, безопасность, конфиденциальность и доступность).	Поставщик обязан получить сертификат ISO 27001 в течение 120 Дней после даты вступления в силу Документа по Транзакции* или Предполагаемой даты** и впоследствии продлевать сертификат на основе оценки авторитетного независимого аудитора каждые 12 месяцев (каждый раз сертификат должен продлеваться для самой последней версии стандарта). Поставщик обязуется получить отчет SOC 2 Типа 2 в течение 240 Дней после даты вступления в силу Документа по Транзакции* или Предполагаемой даты** и впоследствии получать новый отчёт авторитетного независимого аудитора, отражающий результаты проверки систем, средств управления и операций Поставщика в соответствии с SOC 2 Типа 2 (включая, по меньшей мере, безопасность, конфиденциальность и доступность) каждые 12 месяцев. * Если с даты вступления в силу Поставщик предоставляет Размещённую Услугу. ** Дата, начиная с которой Поставщик берёт на себя обязательства по предоставлению Размещённой Услуги.

1.2 Если Поставщик запросит в письменной форме, а Kyndryl разрешит в письменной форме, Поставщик может получить эквивалентный по существу сертификат или отчёт с пониманием того, что периоды времени, указанные в таблице выше, будут применяться без изменения в отношении эквивалентного по существу сертификата или отчёта.

1.3 Поставщик обязуется: (a) по запросу немедленно предоставлять Kyndryl копии любых сертификатов и отчётов, которые Поставщик обязан получить; и (b) немедленно устранять все недостатки внутреннего контроля, обнаруженные во время проверок по SOC 2 или эквивалентному по существу стандарту (если это будет разрешено Kyndryl).

Статья X, Содействие, Проверка и Устранение последствий

Данная Статья применяется, если Поставщик предоставляет Kyndryl Услуги или Поставляемые материалы.

1. Содействие Поставщика

1.1. Если у Kyndryl возникнут вопросы по поводу того, могут ли какие-либо Услуги или Поставляемые материалы в прошлом, настоящем или будущем оказывать влияние на любые проблемы в сфере кибербезопасности, Поставщик обязуется оказать Kyndryl разумное содействие в проведении любых расследований по таким вопросам, в том числе своевременно и полно отвечать на запросы информации, будь то в форме документов, других учётных данных, опросов соответствующего Персонала Поставщика и тому подобного.

1.2. Стороны договорились: (a) предоставлять такую дополнительную информацию друг другу по запросу, (b) подписывать и доставлять друг другу такие прочие документы и (c) выполнять прочие действия, которые может разумно запрашивать другая сторона в целях реализации предназначения данных Положений и документов, упоминаемых в данных Положениях. Например, по запросу Kyndryl Поставщик обязуется оперативно предоставить относящиеся к конфиденциальности и безопасности положения своих письменных договоров с Подрядчиками обработчика и субподрядчиками, в том числе, если у Поставщика есть такое право, путём предоставления доступа непосредственно к договорам.

1.3. По запросу Kyndryl Поставщик оперативно предоставит информацию о странах, в которых его Поставляемые материалы и компоненты этих Поставляемых материалов были произведены, разработаны или получены иным способом.

2. Проверка (в нижеследующем тексте «Объект» означает физическое место, в котором Поставщик размещает и обрабатывает Материалы Kyndryl и осуществляет доступ к ним).

2.1. Поставщик обязуется вести подлежащие аудиту учётные документы, демонстрирующие соблюдение настоящих Положений.

2.2. Kyndryl, самостоятельно или с привлечением внешнего аудитора, имеет право, направив Поставщику предварительное письменное уведомление за 30 Дней, проверить соблюдение Поставщиком настоящих Положений, включая получение доступа к любому Объекту или Объектам с этой целью, притом что Kyndryl не будет получать доступ к любым центрам обработки данных, в которых Поставщик Обрабатывает Данные Kyndryl, если только у Kyndryl не будет объективных оснований полагать, что это может предоставить релевантную информацию. Поставщик обязуется оказывать содействие проверке со стороны Kyndryl, и в том числе своевременно и полно отвечать на запросы информации, будь то в форме документов, других учётных данных, опросов соответствующего Персонала Поставщика и тому подобного. Поставщик может направить на рассмотрение Kyndryl доказательство соблюдения утверждённых норм поведения или утверждённого механизма отраслевой сертификации либо иным способом предоставить Kyndryl информацию для демонстрации соблюдения настоящих Положений.

2.3. Проверка не будет проводиться чаще, чем раз в любой период в 12 месяцев, кроме случаев, когда: (a) Kyndryl проверяет результаты устранения Поставщиком замечаний по итогам предыдущей проверки, проведённой в период в 12 месяцев, или (b) произошло Нарушение безопасности, и Kyndryl желает проверить соблюдение обязательств, имеющих отношение к нарушению. В любом случае Kyndryl направит такое же письменное уведомление за 30 Дней, как указано в Разделе 2.2 выше, однако потребность в оперативном устранении последствий Нарушения безопасности может потребовать от Kyndryl проверки с письменным уведомлением меньше, чем через 30 Дней.

2.4. Регулирующий орган или другой Оператор может реализовать те же права, что Kyndryl, предусмотренные Разделами 2.2 и 2.3, причем регулирующий орган также может реализовать дополнительные права, которые предоставлены ему законом.

2.5. Если у Kyndryl возникнут разумные основания полагать, что Поставщик не соблюдает любые из этих Положений (независимо от того, возникнут ли эти основания в результате проверки согласно настоящим Положениям или по другой причине), Поставщик обязуется оперативно устранить последствия такого несоблюдения.

3. Программа борьбы с контрафактом

3.1. Если Поставляемые материалы Поставщика содержат электронные компоненты (например, жёсткие диски, твердотельные накопители, память, процессоры, логические устройства или кабели), Поставщик обязуется развернуть и соблюдать документированную программу борьбы с контрафактом, направленную прежде всего на предотвращение поставки Поставщиком контрафактных компонентов компании Kyndryl, а также на оперативное обнаружение и устранение последствий ситуаций, в которых Поставщик непреднамеренно поставляет контрафактные компоненты компании Kyndryl. Поставщик обязуется установить такое же обязательство по развёртыванию и соблюдению документированной программы борьбы с контрафактом на всех своих поставщиков, поставляющих электронные компоненты, входящие в Поставляемые материалы Поставщика, поставляемые компании Kyndryl.

4. Устранение последствий

4.1. Если Поставщик нарушит любые обязательства, установленные для него настоящими Положениями, и такое нарушение приведёт к Нарушению безопасности, Поставщик обязуется устранить нарушение и устранить негативные последствия Нарушения безопасности в соответствии с разумными указаниями и графиком, установленными Kyndryl. Однако, если Нарушение безопасности возникает в результате предоставления Поставщиком Размещённой услуги с множественной арендой и, как следствие, охватывает нескольких заказчиков Поставщика, включая Kyndryl, то Поставщик должен, с учётом типа Нарушения безопасности, своевременно и надлежащим образом исправить сбой и устранить негативные последствия Нарушения безопасности, предоставив Kyndryl возможность рассмотрения действий по исправлению и устранению последствий.

4.2. Kyndryl имеет право на участие в процессе устранения Нарушения безопасности в соответствии с Разделом 4.1 в объёме по своему усмотрению, и Поставщик будет нести ответственность за свои издержки и расходы, связанные с устранением нарушения, и за издержки и расходы обеих сторон, связанные с устранением последствий любого такого Нарушения безопасности.

4.3. Например, в состав издержек, связанных с устранением последствий Нарушения безопасности, могут входить издержки на обнаружение и расследование Нарушения безопасности, определение обязанностей, установленных применимыми законами и нормами, создание и обслуживание контактных центров, предоставление услуг кредитного мониторинга и восстановления кредитной истории, повторную загрузку данных, исправление дефектов в продуктах (в том числе путём разработки Исходного Кода и иной разработки), привлечение третьих лиц к содействию в вышеперечисленной и другой деятельности, а также прочие издержки и расходы, необходимые для устранения негативных последствий Нарушения безопасности. Во избежание разночтений: в состав издержек на устранение последствий не входят упущенная прибыль, возможность проведения деловой активности, потерянная стоимость, выручка, деловая репутация и ожидаемые сбережения Kyndryl.