Член I, Информация за служебни контакти

Този Член е в сила, ако Доставчикът или Kyndryl Обработва ИСК на съответната друга страна.

1.1 Kyndryl и Доставчикът могат да Обработват ИСК на другата страна, когато извършват бизнес дейности във връзка с предоставянето от Доставчика на Услуги и Продукти.

1.2 Дадена страна:

a) няма да използва или разкрива ИСК на другата страна с каквато и да е друга цел (уточнение: нито една от страните не Продава ИСК на другата, нито използва или разкрива ИСК на другата за каквато и да е маркетингова цел без предварителното писмено съгласие на другата страна, а при необходимост – и без предварително писмено съгласие на засегнатите Субекти на данни), и

b) изтрива, променя, коригира, връща, предоставя информация за Обработването, ограничава Обработването или предприема други разумни действия по отношение на ИСК на другата незабавно при писмено искане от другата страна.

1.3 Страните не влизат във взаимоотношения на съвместни Администратори по отношение на ИСК на всяка от страните и нито една разпоредба от Документа по сделката няма да бъде тълкувана или приемана като индикация за намерение за установяване на взаимоотношения на съвместни Администратори.

1.4 Заявлението за поверителност на Kyndryl на адрес https://www.kyndryl.com/privacy съдържа допълнителни подробности за Обработването на ИСК от Kyndryl.

1.5 Страните са предприели и ще поддържат технически и организационни мерки за сигурност, за да защити ИСК на другата страна от загуба, унищожаване, промяна, случайно или неправомерно разкриване, случаен или неправомерен достъп и незаконно Обработване.

1.6 Доставчикът уведомява Kyndryl незабавно (и в никакъв случай не по-късно от 48 часа), след като установи Нарушение на сигурността, касаеща ИСК на Kyndryl. Доставчикът ще извършва това уведомяване чрез Портала на Kyndryl за глобално съдействие за доставките нahttps://www.kyndryl.com/procurement/procSupport. Доставчикът предоставя на Kyndryl основателно поискана информация за подобно нарушение и за състоянието на всички мерки, предприети от Доставчика по отстраняване и възстановяване. Тази основателно поискана информация може да включва например регистрационни файлове, съдържащи данни за привилегирован, административен и друг достъп до Устройства, системи или приложения, точни копия на Устройства, системи или приложения и други подобни елементи до степента, отнасяща се до нарушението или до дейностите на Доставчика по отстраняване и възстановяване.

1.7 Когато Доставчикът обработва ИСК само на Kyndryl и няма достъп до каквито и да било други данни или материали или до каквато и да е корпоративна система на Kyndryl, този Член и Член X (Сътрудничество, проверка и възстановяване) са единствените членове, които се прилагат за това Обработване.

Член II, Технически и организационни мерки, Сигурност на данните

Този Член е в сила, когато Доставчикът Обработва Данни на Kyndryl, различни от ИСК на Kyndryl. Доставчикът спазва изискванията на този Член при предоставянето на всички Услуги и Продукти и по този начин защитава Данни на Kyndryl от загуба, унищожаване, промяна, неволно или неразрешено разкриване, случаен или неразрешен достъп и незаконно Обработване. Изискванията на този Член се отнасят за всички ИТ приложения, платформи и инфраструктура, които Доставчикът използва или управлява при предоставянето на Продукти и Услуги, включително всички разработки, тествания, хостинг, поддръжка, операции и среди на центровете за данни.

1. Употреба на данни

1.1. Доставчикът няма право да добавя към Данните на Kyndryl или да включва към Данните на Kyndryl каквато и да е друга информация или данни, включително всякакви Лични данни, без предварително писмено съгласие на Kyndryl. Доставчикът няма право също да използва Данни на Kyndryl под каквато и да е форма, обобщена или по друг начин, за каквато и да е друга цел, освен за предоставянето на Услуги и Продукти (на Доставчика не е позволено например да използва или повторно да използва Данни на Kyndryl за оценка на ефективността или средствата за подобряване на офертите на Доставчика, за изследвания и разработки за създаване на нови оферти или за генериране на отчети относно офертите на Доставчика). Освен ако изрично не е разрешено в Документа по сделката, Доставчикът няма право да Продава Данни на Kyndryl.

1.2. Доставчикът няма да вгражда никакви технологии за уеб проследяване в Продуктите или като част от Услугите (такива технологии включват HTML5, локално съхранение, маркери или кодове на трети страни и уеб маяци), освен ако това не е изрично разрешено в Документа по сделката.

2. Искания на трети страни и Поверителност

2.1. Доставчикът няма да разкрива Данни на Kyndryl пред която и да е трета страна, освен ако не получи предварително писмено разрешение от Kyndryl за това. Ако правителство, включително регулаторен орган, изисква достъп до Данни на Kyndryl (например, ако правителството на САЩ връчи на Доставчика заповед във връзка с националната сигурност за получаване на Данни на Kyndryl) или ако разкриването на Данни на Kyndryl се изисква по друг начин по закон, Доставчикът уведомява писмено Kyndryl за такова искане или изискване и предоставя на Kyndryl разумна възможност да оспори всяко разкриване (когато законът забранява уведомяването, Доставчикът предприема стъпките, които разумно счита за подходящи, за да оспори забраната и разкриването на Данни на Kyndryl чрез съдебни действия или други средства).

2.2. Доставчикът уверява Kyndryl, че: а) само онези от неговите служители, които се нуждаят от достъп до Данни на Kyndryl, за да предоставят Услуги или Продукти, получават този достъп и то само до степента, необходима за предоставяне на тези Услуги и Продукти; и б) е обвързал служителите си със задълженията за поверителност, които изискват тези служители да използват и разкриват Данни на Kyndryl само съгласно изискванията на настоящите Условия.

3. Връщане или изтриване на Данни на Kyndryl

3.1. По искане на Kyndryl Доставчикът изтрива или връща Данните на Kyndryl на Kyndryl след прекратяване или изтичане на Документа по сделката или по-рано при поискване от Kyndryl. Ако Kyndryl изисква изтриване, тогава Доставчикът, в съответствие с Най-добрите индустриални практики, прави данните нечетливи и ги обработва така, че да не могат да бъдат повторно обобщени или възстановени, и удостоверява изтриването пред Kyndryl. Ако Kyndryl изисква връщането на Данни на Kyndryl, то тогава Доставчикът прави това по график, установен от Kyndryl, и съгласно разумните писмени указания на Kyndryl.

Член III, Поверителност

Този Член важи, когато Доставчикът обработва Лични данни на Kyndryl.

1. Обработване

1.1 Kyndryl определя Доставчика за Обработващ във връзка с Обработването на Лични данни на Kyndryl с единствената цел да предостави Продуктите и Услугите в съответствие с инструкциите на Kyndryl, включително съдържащите се в тези Условия, Документа по сделката и свързания основен договор между страните. Ако Доставчикът не спази някоя инструкция, Kyndryl може да прекрати съответната част от Услугите с писмено предизвестие. Ако Доставчикът смята, че дадена инструкция нарушава закон за защита на данните, Доставчикът уведомява Kyndryl незабавно и в рамките на определените от закона срокове.

1.2 Доставчикът спазва всички закони за защита на данните, приложими за Услугите и Продуктите.

1.3 В Приложение към Документа по сделката или в самия Документ по сделката е изложено следното във връзка с Данните на Kyndryl:

(a) категории Субекти на данни;
(b) типове Лични данни на Kyndryl;
(c) действия с данни и дейности по Обработване;
(d) времетраене и честота на Обработване; и
(e) списък с Подизпълнители, обработващи лични данни.

2. Технически и организационни мерки

2.1 Доставчикът прилага и поддържа техническите и организационните мерки, заложени в Член II (Технически и организационни мерки, Сигурност на данните) и Член VIII (Технически и организационни мерки, Обща сигурност), като по този начин гарантира ниво на сигурност, съответстващо на риск, свързан с Услугите и Продуктите. Доставчикът удостоверява и разбира ограниченията, предвидени в Член II, този Член III и Член VIII и ги спазва.

3. Права и искания на Субекта на данни

3.1 Доставчикът информира Kyndryl незабавно (по график, който позволява на Kyndryl и всеки друг Администратор да изпълнява своите законни задължения) за всяко искане от Субект на данни за упражняване на каквито и да е права на Субекта на данни (напр. коригиране, изтриване или блокиране на данни) относно Лични данни на Kyndryl. Доставчикът може също без отлагане да насочи Субект на данни, който е отправил подобно искане, към Kyndryl. Доставчикът няма да отговаря на искания от Субекти на данни, освен ако не е правно задължен или Kyndryl му е дала писмено указание да направи това.

3.2 Ако Kyndryl е задължено да предостави информация относно Лични данни на Kyndryl на други Администратори или други трети страни (например Субекти на данни или регулатори), Доставчикът помага на Kyndryl, като предоставя информация и предприема други разумни действия, които се изискват от Kyndryl, по график, който позволява на Kyndryl своевременно да реагира на тези други Администратори или трети страни.

4. Подобработващи

4.1 Доставчикът уведомява Kyndryl чрез предварително писмено известие преди добавяне на нов Подобработващ или разширяване на обхвата на Обработването за съществуващ Подобработващ, като в това писмено известие се посочва името на Подобработващия и се описва новият или разширен обхват на Обработване. Kyndryl има право по всяко време да отправи основателно

възражение срещу всеки такъв нов Подобработващ или разширен обхват по разумни причини, като ако това стане, страните работят заедно добросъвестно по възражението на Kyndryl. Предвид правото на Kyndryl да отправя възражения по всяко време Доставчикът може да наеме новия Подобработващ или да разшири обхвата на Обработването на съществуващия Подобработващ, ако Kyndryl не подаде възражение в рамките на 30 дни от датата на писменото известие на Доставчика.

4.2 Доставчикът изисква спазване на задълженията за защита на данните, сигурността и сертифицирането, посочени в тези Условия, от всеки одобрен Подобработващ, преди този Подобработващ да Обработва Данни на Kyndryl. Доставчикът носи пълна отговорност пред Kyndryl за изпълнение на задълженията на всеки Подобработващ.

5. Трансгранично Обработване на Данни

Дефиниции на термините, използвани по-долу:

Държава с адекватно ниво на защита означава държава, която осигурява адекватно ниво на защита на данните по отношение на съответното прехвърляне съгласно приложимото законодателство за защита на данните или решения на регулатори.

Вносител на данни означава или Обработващ, или Подобработващ, който не е установен в Държава с адекватно ниво на защита.

Стандартни договорни клаузи на ЕС („СДК на ЕС“) означава Стандартните договорни клаузи на ЕС (Решение 2021/914 на Комисията) с приложени незадължителни клаузи, с изключение на вариант 1 на Клауза 9(а) и вариант 2 от Клауза 17, както са публикувани официално на https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en.

Стандартни договорни клаузи на Сърбия („СДК на Сърбия“) означава Стандартните договорни клаузи на Сърбия, както са приети от „Сръбския комисар по информацията от обществено значение и защитата на личните данни“, публикувани на https://www.poverenik.rs/images/stories/dokumentacija-nova/podzakonski-akti/Klauzulelat.docx.

Стандартни договорни клаузи („**СДК**“) означава договорните клаузи, които се изискват от приложимите законодателства за защита на данните, за прехвърляне на Лични данни на Обработващи, които не са установени в Държави с адекватно ниво на защита.

Стандартни договорни клаузи на Обединеното кралство („СДК на Обединеното кралство“) означава Стандартните договорни клаузи на Обединеното кралство за Администратори към Обработващи, както са публикувани официално наhttps://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers-after-uk-exit/sccs-after-transition-period/.

5.1 Доставчикът няма да осъществява трансгранично прехвърляне или разкриване (включително чрез отдалечен достъп) на каквито и да са Лични данни на Kyndryl без предварителното писмено съгласие на Kyndryl. Ако Kyndryl даде такова съгласие, страните си сътрудничат, за да се гарантира спазване на приложимите законодателства за защита на данните. Ако СДК се изискват съгласно тези закони, Доставчикът незабавно приема СДК по искане на Kyndryl.

5.2 Що се отнася до СДК на ЕС:

(a) Ако Доставчикът не е установен в Държава с адекватно ниво на защита: Доставчикът с настоящото сключва СДК на ЕС като Вносител на данни с Kyndryl и Доставчикът ще сключи писмени договори с всеки одобрен Подобработващ съгласно Клауза 9 от СДК на ЕС и ще предостави на Kyndryl копия от тези договори при поискване.

(I) Модул 1 от СДК на ЕС не е приложим, освен ако страните не уговорят писмено друго.

(II) Модул 2 от СДК на ЕС е приложим, когато Kyndryl е Администратор, а Модул 3 е приложим, когато Kyndryl е Обработващ. Съгласно Клауза 13 от СДК на ЕС, когато са приложими Модули 2 или 3, страните се съгласяват, че (1) СДК на ЕС ще се ръководят от законодателството на държавата членка на ЕС, където се намира компетентният надзорен орган, и (2) споровете, произтичащи от СДК на ЕС, ще се решават от съдилищата на държавата членка на ЕС, където се намира компетентният надзорен орган. Ако законодателството в (1) не предвижда права на трети страни бенефициери, СДК на ЕС ще се ръководят от законодателството на Нидерландия и споровете, произтичащи от СДК на ЕС съгласно (2), ще се решават от съда в Амстердам, Нидерландия.

(b) Ако Доставчикът е установен в Европейското икономическо пространство и Kyndryl е Администратор, който не е подчинен на Общия регламент относно защитата на данните 2016/679, приложим е Модул 4 от СДК на ЕС, и Доставчикът с настоящото сключва СДК на ЕС като износител на данни с Kyndryl. Ако е приложим Модул 4 от СДК на ЕС, страните се съгласяват, че СДК на ЕС ще се ръководят от законодателството на Нидерландия и споровете, произтичащи от СДК на ЕС, ще се решават от съда в Амстердам, Нидерландия.

(c) Ако други администратори, напр. Клиенти или свързани лица поискат да станат страна по СДК на ЕС съгласно „клаузата за присъединяване“ от Клауза 7, с настоящото Доставчикът дава съгласие за всяко подобно искане.

(d) Техническите и организационните мерки, необходими за попълване на приложение II към СДК на ЕС, са описани в тези Условия, Документа по сделката и свързания основен договор между страните.

(e) В случай на противоречие между СДК на ЕС и тези Условия предимство имат СДК на ЕС.

5.3 Що се отнася до СДК на Обединеното кралство:

(a) Ако Доставчикът не е установен в Държава с адекватно ниво на защита: (I) Доставчикът от свое име като Вносител на данни с настоящото сключва СДК на Обединеното кралство с Kyndryl и (II) Доставчикът ще сключи писмени договори с всеки одобрен Подобработващ, който е Вносител на данни съгласно Клауза 11 от СДК на Обединеното кралство и ще предостави на Kyndryl копия от тези договори при поискване.

(b) Ако Доставчикът е установен в Държава с адекватно ниво на защита, тогава Доставчикът с настоящото сключва СДК на Обединеното кралство с Kyndryl от името на всеки Подобработващ, който е Вносител на данни. Ако Доставчикът е в невъзможност да осигури това за някой Подобработващ, Доставчикът ще предостави на Kyndryl СДК на Обединеното кралство, подписани от този Подобработващ, за насрещно подписване от Kyndryl, преди да позволи на Подобработващия да Обработва Лични данни на Kyndryl.

(c) СДК на Обединеното кралство между Kyndryl и Доставчик ще служат или като СДК на Обединеното кралство между Администратор и Обработващ, или като насрещен писмен договор между „вносител на данни“ и „подобработващ“ в съответствие с Клауза 11 от СДК на Обединеното

кралство, както се налага от обстоятелствата. В случай на противоречие между СДК на Обединеното кралство и тези Условия предимство имат СДК на Обединеното кралство.

(d) Други Администратори, напр. Клиенти или свързани лица, може да поискат да станат допълнителни „износители на данни“. Доставчикът се съгласява от свое име и от името на своите Подобработващи с всяко такова искане. Kyndryl ще уведоми Доставчика за евентуални допълнителни „износители на данни“ и, на свой ред, Доставчикът ще уведоми своите Подобработващи за тези допълнителни „износители на данни“.

5.4 Що се отнася до СДК на Сърбия:

(a) Ако Доставчикът не е установен в Държава с адекватно ниво на защита: (I) Доставчикът от свое име като Обработващ с настоящото сключва СДК на Сърбия с Kyndryl и (II) Доставчикът ще сключи писмени договори с всеки одобрен Подобработващ лични данни, съгласно Клауза 8 от СДК на Сърбия и ще предостави на Kyndryl копия от тези договори при поискване.

(b) Ако Доставчикът е установен в Държава с адекватно ниво на защита, тогава той с настоящото сключва СДК на Сърбия с Kyndryl от името на всеки Подобработващ, намиращ се в държава, различна от Държава с адекватно ниво на защита. Ако Доставчикът не бъде в състояние да стори това с който и да било Подобработващ, Доставчикът ще предостави на Kyndryl СДК на Сърбия, подписани от този Подобработващ, за насрещно подписване от Kyndryl преди да позволи на Подобработващия да обработва Лични данни на Kyndryl.

(c) СДК на Сърбия между Kyndryl и Доставчик ще служат или като СДК на Сърбия между Администратор и Обработващ, или като насрещен писмен договор между „обработващ“ и „подобработващ“, както се налага от обстоятелствата. В случай на противоречие между СДК на Сърбия и тези Условия, предимство имат СДК на Сърбия.

(d) Информацията, изискваща се за попълване на приложения 1 до 8 към СДК на Сърбия за уреждането на прехвърляне на Лични данни в държава, различна от Държава с адекватно ниво на защита, може да бъде намерена в тези Условия и в Приложение към Документа по сделката, или в самия Документ по сделката.

6. Съдействие и документиране

6.1 Като взема предвид естеството на Обработването, Доставчикът помага на Kyndryl, като въвежда подходящи технически и организационни мерки за изпълнение на задължения, свързани със заявки и права на Субектите на данни. Доставчикът помага на Kyndryl при гарантиране спазването на задълженията, свързани със сигурността на Обработването, уведомяването и известяването за Нарушение на сигурността и създаването на оценки за въздействието върху защитата на личните данни, включително предварителна консултация с отговорния регулаторен орган, ако е необходимо, като взема предвид информацията, с която Доставчикът разполага.

6.2 Доставчикът поддържа актуален запис на името и данните за контакт на всеки Подобработващ, включително на всеки представител на Подобработващ и длъжностно лице по защита на данните. При поискване Доставчикът предоставя този запис на Kyndryl по график, който позволява на Kyndryl своевременно да отговори на всяко искане от Клиент или друга трета страна.

Член IV, Технически и организационни мерки, Сигурност на кодовете

Този Член важи, ако Доставчикът има достъп до Първичен код на Kyndryl. Доставчикът спазва изискванията на този Член и по този начин защитава Първичния код на Kyndryl от загуба, унищожаване, промяна, неволно или неразрешено разкриване, случаен или неразрешен достъп и незаконно Боравене. Изискванията на този Член се отнасят за всички ИТ приложения, платформи и инфраструктура, които Доставчикът използва или управлява при предоставянето на Продукти и Услуги и при Боравенето с Технологии на Kyndryl, включително всички разработки, тествания, хостинг, поддръжка, операции и среди на центровете за данни.

1. Изисквания за сигурност

Дефиниции на термините, използвани по-долу:

Забранена държава означава всяка държава, която: а) американското правителство е определило като чуждестранен противник съгласно Изпълнителната заповед за Осигуряване на веригата на доставки за информационни и комуникационни технологии и услуги от 15 май 2019 г.; б) е включена в списък съгласно раздел 1654 от Закона за национално разрешение за отбрана на САЩ от 2019 г.; или в) е идентифицирана като „Забранена държава“ в Документа по сделката.

1.1. Доставчикът няма да разпространява или поставя Първичен код на Kyndryl за доверителна употреба в полза на трета страна.

1.2. Доставчикът няма да разрешава какъвто и да е Първичен код на Kyndryl да се съхранява на сървъри, намиращи се в Забранена държава. Доставчикът няма да разрешава на никого, включително на своя Персонал, намиращ се в Забранена държава или посещаващ Забранена държава (за продължителността на всяко такова посещение), по каквато и да е причина, да има достъп или да използва който и да е Първичен код на Kyndryl, независимо дали този Първичен Код на Kyndryl има глобално разположение, както и няма да позволява разработването, тестването или друга дейност в Забранена държава, които биха изисквали такъв достъп или употреба.

1.3. Доставчикът няма да поставя или разпространява Първичен код на Kyndryl в юрисдикция, в която законът или тълкуването на закона изисква разкриване на Първичен код на трета страна. Ако има промяна в закона или тълкуването на закона в юрисдикцията, в която се намира Първичен код на Kyndryl, което може да наложи изискването Доставчикът да разкрие този Първичен код на трета страна, Доставчикът незабавно трябва да унищожи или премахне Първичния код на Kyndryl от тази юрисдикция и да не поставя никакви други Първични кодове на Kyndryl в тази юрисдикция, ако такъв закон или тълкуване на закон останат в сила.

1.4. Доставчикът няма, пряко или косвено, да предприема действия, включително да сключва какъвто и да е договор, които биха довели до това Доставчикът, Kyndryl или която и да е трета страна да поеме задължение за разкриване съгласно Раздели 1654 или 1655 от Закона за национално разрешение за отбрана на САЩ от 2019 г. За по-голяма яснота, освен ако не е изрично разрешено в Документа по сделката или свързания основен договор между страните, Доставчикът няма право при никакви обстоятелства да разкрива Първичен код на Kyndryl пред трета страна без предварителното писмено съгласие на Kyndryl.

1.5. Ако Kyndryl уведоми Доставчика или трета страна уведоми която и да е от страните, че: (a) Доставчикът е позволил Първичен код на Kyndryl да бъде внесен в Забранена страна или която и да е юрисдикция, посочена в Раздел 1.3 по-горе, (b) Доставчикът по друг начин е разпространил, достъпил или използвал Първичен код на Kyndryl по начин, който не е позволен в Документа по сделката или свързан основен или друг договор между страните или (c) Доставчикът е нарушил Раздел 1.4 по-горе, тогава без да се ограничават правата на Kyndryl съгласно закона или справедливостта, или съгласно Документа по сделката, или свързан основен или друг договор между страните: (I) ако подобно уведомление е връчено до Доставчика, то Доставчикът незабавно известява Kyndryl за него; и (II) Доставчикът, като следва разумните

указания на Kyndryl, разследва и разрешава въпроса по план, надлежно определен от Kyndryl (след консултации с Доставчика).

1.6. Ако Kyndryl основателно смята, че са необходими промени в политиките, процедурите, контрола или практиките на Доставчика във връзка с достъпа до Първичния код с цел справяне с киберсигурността, кражбите на интелектуална собственост или подобни или свързани рискове (включително риска без такива промени Kyndryl да не може да продава на определени Клиенти или на определени пазари или по друг начин да не може да удовлетвори изискванията за сигурност или веригата на доставките на Клиента), то тогава Kyndryl може да се свърже с Доставчика, за да обсъдят действията, необходими за справяне с подобни рискове, включително промените в съответните политики, процедури, контроли или практики. По искане на Kyndryl Доставчикът си сътрудничи с Kyndryl при извършването на оценка за необходимостта от подобни промени, както и при въвеждането на подходящи взаимно съгласувани промени.

Член V, Сигурни разработки

Настоящият Член е приложим ако Доставчикът ще предостави свой или на трета страна Софтуер на място на Kyndryl или ако Продуктите или Услугите на Доставчика ще бъдат предоставени на Клиент на Kyndryl като част от продукт или услуга на Kyndryl.

1. Готовност за сигурност

Доставчикът си сътрудничи с вътрешните процеси на Kyndryl, които оценяват готовността за сигурност на продуктите и услугите на Kyndryl, зависещи от Продуктите на Доставчика, включително чрез навременна и ефективна реакция на заявки за информация, независимо дали чрез документи, други записи, интервюта на съответния Персонал на Доставчика, или други подобни.

2. Сигурни разработки

2.1 Настоящият Раздел 2 е приложим само когато Доставчикът предоставя Софтуер на място на Kyndryl.

2.2 Доставчикът е внедрил и ще поддържа през целия срок на Документа по сделката, съгласно Най-добрите индустриални практики мрежа, платформа, система, приложения, устройства, физическа инфраструктура, реакция при инциденти и ориентирани към Персонала политики, процедури и мерки за контрол по сигурността, които са необходими за защита на: (a) системите и средата за разработка, изграждане, изпитване и операции, които Доставчикът или трета страна, ангажирана от Доставчика, експлоатира, управлява, ползва или на които другояче разчита за или по отношение на Продукти и (b) всички първични кодове на Продукти от загуба, незаконни форми на боравене или неразрешен достъп, разкриване или изменение.

3. Уязвимости в сигурността

3.1 Настоящият Раздел 3 е приложим само ако Продукти или Услуги на Доставчика ще бъдат предоставени на Клиент на Kyndryl като част от продукт или услуга на Kyndryl.

3.2 Доставчикът придобива сертификат за съответствие с ISO 20243, Information technology, Open Trusted Technology Provider™ Standard (O-TTPS), Mitigating maliciously tainted and counterfeit products [Информационни технологии, стандарт Open Trusted Technology Provider™, Противодействие на злонамерени и фалшифицирани продукти] (чрез самооценка или въз основа на оценка, извършена от компетентен независим одитор). Алтернативна възможност е Доставчикът да заяви писмено, а Kyndryl да даде писмено одобрение, Доставчикът да получи сертификат за съответствие с по същество еквивалентен индустриален стандарт, касаещ надеждни практики за разработване и за веригата на доставките (сертифициране чрез самооценка или базирано на оценката на компетентен независим одитор съгласно изискванията на Kyndryl).

3.3 Доставчикът придобива сертификат за съответствие с ISO 20243 или с по същество еквивалентен индустриален стандарт (след писмено одобрение от страна на Kyndryl) до 180 дни след влизането в сила на Документа по сделката, като след това сертификатът се подновява на всеки 12 месеца (всяко подновяване се прави в съответствие с най-актуалната версия на приложимия стандарт, т.е. ISO 20243, или когато Kyndryl е одобрила писмено, принципно еквивалентен индустриален стандарт, отнасящ се до сигурните практики за разработване и за веригата на доставките).

3.4 При поискване Доставчикът незабавно предоставя на Kyndryl копие от сертификатите, които Доставчикът е длъжен да придобие съгласно раздели 2.1 и 2.2 по-горе.

4. Уязвимости в сигурността

Дефиниции на термините, използвани по-долу:

Коригиране на грешки означава корекция и проверка на пропуски с цел отстраняване на грешки или недостатъци, включително Уязвимости в сигурността, от Продуктите.

Противодействие означава прилагане на изпитани средства за ограничаване или избягване на рисковете от Уязвимост в сигурността.

Уязвимост в сигурността означава състояние в проектирането, кодирането, разработването, внедряването, тестването, експлоатацията, съдействието, поддръжката или управлението на даден Продукт, който позволява атака от страна на който и да било, която може да доведе до неправомерен достъп или експлоатация, включително: а) достъп до, контрол или прекъсване на работата на система; б) достъп до, изтриване, промяна или извличане на данни; или в) промени в идентичността, удостоверяване или разрешения на потребители или администратори. Уязвимост в сигурността може да съществува независимо от това дали има присвоена идентификация за Общи уязвимости и експозиции (CVE), някаква оценка или официална класификация.

4.1 Доставчикът заявява и гарантира, че ще: а) използва Най-добрите индустриални практики, за да идентифицира Уязвимости в сигурността, включително чрез непрекъснато статично и динамично сканиране на сигурността на приложението на първичен код, сканиране на сигурността на отворен първичен код и сканиране на пропуските в системата; и б) спазва изискванията на тези Условия, за да предотврати, установи и коригира Уязвимости в сигурността на Продуктите и всички IT приложения, платформи и инфраструктура, и в които и чрез които Доставчикът създава и предоставя Услуги и Продукти.

4.2 Ако Доставчикът установи Уязвимост в сигурността на даден Продукт или ИТ приложение, платформа или инфраструктура, Доставчикът предоставя на Kyndryl Корекция на грешките и Мерки за противодействие за всички версии на Продуктите в съответствие с Нивата на сериозност и времевите рамки, посочени в таблиците по-долу:

Ниво на сериозност*
Извънредна Уязвимост в сигурността – Уязвимост в сигурността, която представлява сериозна и потенциално глобална заплаха. Kyndryl определя Извънредните Уязвимости в сигурността по свое усмотрение, независимо от базовия рейтинг на CVSS.
Критична – Уязвимост в сигурността, която има базов рейтинг на CVSS от 9 до 10,0
Висока – Уязвимост в сигурността, която има базов рейтинг на CVSS от 7,0 до 8,9
Средна – Уязвимост в сигурността, която има базов рейтинг на CVSS от 4,0 до 6,9
Ниска – Уязвимост в сигурността, която има базов рейтинг на CVSS от 0,0 до 3,9

Срокове				
Извънреден	***Критичен***	***Висок***	***Среден***	***Нисък***
До 4 дни, както е посочено от Главното бюро по информационна сигурност на Kyndryl	30 дни	30 дни	90 дни	Съгласно Най-добрите индустриални практики

* Във всеки случай, когато няма посочен базов рейтинг на CVSS за Уязвимост в сигурността, Доставчикът прилага Ниво на сериозност, което е подходящо за естеството и обстоятелствата на съответния пробив.

4.3 При Уязвимост в сигурността, която е била разкрита публично и за която Доставчикът все още не е предоставил на Kyndryl никаква Корекция на грешки или Мерки за противодействие, Доставчикът трябва да приложи всякакви технически изпълними допълнителни контроли за

сигурност, които смекчават рисковете от уязвимостта.

4.4 Ако Kyndryl не е удовлетворено от мерките на Доставчика срещу конкретна Уязвимост в сигурността на даден Продукт или приложение, платформа или инфраструктура, посочени по-горе, то тогава, без да се засягат други права на Kyndryl, Доставчикът незабавно организира обсъждане на проблемите директно между Kyndryl и вицепрезидент на Доставчика или друг съответен представител на ръководството, отговарящ за Корекция на грешките.

4.5 Примерите за Уязвимост в сигурността включват код на трета страна или отворен първичен код за край на услугата (EOS), за които вече не се получават корекции на защитата.

Член VI, Достъп до корпоративни системи

Този Член важи, ако служители на Доставчика имат достъп до която и да е Корпоративна система.

1. Общи условия

1.1 Kyndryl определя дали да разреши на служителите на Доставчика достъп до Корпоративните системи. Ако Kyndryl разреши достъпа, Доставчикът ще спазва и ще осигури неговите служители, които осъществяват достъпа, да спазват изискванията на настоящия Член.

1.2 Kyndryl определя начините, по които служителите на Доставчика могат да осъществяват достъп до Корпоративните системи, включително дали тези служители ще осъществяват достъп до Корпоративните системи чрез устройства, предоставени от Kyndryl или от Доставчика.

1.3 Служителите на Доставчика могат да осъществяват достъп само до Корпоративни системи и да предоставят Услуги само чрез Устройства, за които Kyndryl предостави разрешение. Служителите на Доставчика нямат право да използват Устройства, които Kyndryl разрешава, за предоставяне на услуги на друго лице или предприятие, нито да осъществяват достъп до ИТ системи, мрежи, приложения, уебсайтове, инструменти за електронна поща, инструменти за сътрудничество или други подобни за или във връзка с Услугите на други Доставчици или трети страни.

1.4 За по-голяма яснота служителите на Доставчика нямат право да използват за лични цели Устройства, които Kyndryl разрешава за достъп до Корпоративните системи (напр. служителите на Доставчика нямат право да съхраняват лични файлове като музика, видеоклипове, снимки или други подобни на тези Устройства, нито да използват интернет от тези устройства за лични цели).

1.5 Служителите на Доставчика нямат право да копират Материали на Kyndryl, достъпни през дадена Корпоративна система, без предварителното писмено одобрение на Kyndryl (и е напълно забранено да копират каквито и да е Материали на Kyndryl на преносимо устройство за съхранение, например USB, външен твърд диск или други подобни устройства).

1.6 При поискване Доставчикът потвърждава, с имена на служителите, до кои специфични Корпоративни системи служителите му са упълномощени да имат достъп и са осъществили достъп в рамките на който и да е период от време, посочен от Kyndryl.

1.7 Доставчика уведомява Kyndryl в рамките на двадесет и четири (24) часа, в случай че който и да е служител на Доставчика с достъп до която и да е Корпоративна система вече не: а) е нает от Доставчика; или б) работи по дейности, изискващи подобен достъп. Доставчикът работи с Kyndryl, за да гарантира, че достъпът на такива бивши или настоящи служители е преустановен незабавно.

1.8 Доставчикът незабавно докладва за действителни или предполагаеми инциденти със сигурността (напр. загуба на устройство на Kyndryl или Доставчика или неразрешен достъп до Устройство или данни, материали или друга информация от какъвто и да е характер) на Kyndryl и си сътрудничи с Kyndryl при разследването на подобни инциденти.

1.9 Доставчикът няма право да разрешава на който и да е агент, независим изпълнител или служител на подизпълнител достъп до която и да е Корпоративна система без предварителното писмено съгласие на Kyndryl; ако Kyndryl предостави такова съгласие, то тогава Доставчикът ангажира чрез договор тези лица и техните работодатели да спазват изискванията на този Член, все едно тези лица са служители на Доставчика, и отговаря пред Kyndryl за всички действия и бездействия от страна на всяко такова лице или работодател по отношение на достъпа до Корпоративните системи.

2. Софтуер на устройството

2.1 Доставчикът дава указания на служителите си своевременно да инсталират на Устройството всеки софтуер, изискван от Kyndryl за улесняване на защитения достъп до Корпоративните

системи. Нито Доставчикът, нито неговите служители възпрепятстват функционирането на софтуера или на защитните функции, които предоставя софтуерът.

2.2 Доставчикът и неговите служители се придържат към правилата за конфигуриране на Устройства, които Kyndryl задава, и си сътрудничат по всякакъв друг начин с Kyndryl, за да гарантират, че функциите на софтуера са според намеренията на Kyndryl. Например Доставчикът няма да отмени функцията за блокиране на уебсайтове или автоматизираните функции за коригиране.

2.3 Служителите на Доставчика нямат право да споделят с когото и да било Устройствата, които използват за достъп до Корпоративните системи, или потребителските имена, пароли или други подобни за тези Устройства.

2.4 Ако Kyndryl упълномощи служителите на Доставчика да получат достъп до корпоративните системи през Устройства на Доставчика, то тогава Доставчикът инсталира и стартира операционна система на онези Устройства, които Kyndryl одобрява, надстройва до нова версия съществуващата операционна система или инсталира нова операционна система в разумен срок след инструктиране от страна на Kyndryl.

3. Надзор и сътрудничество

3.1 Kyndryl има неограничени права да следи и да противодейства на потенциални прониквания и други заплахи за киберсигурността по каквито и да е начини, от каквито и да е места и чрез каквито и да е средства, които Kyndryl счита за необходими или подходящи, без предварително уведомяване на Доставчика, служител на Доставчика или друго лице. Като пример за такива права Kyndryl може по всяко време: а) да извършва тест за защита на което и да е Устройство, б) да наблюдава, възстановява чрез технически или други средства и да следи комуникациите (включително имейли от каквито и да е имейл акаунти), записи, файлове и други елементи, съхранявани в което и да е Устройство или предавани през която и да е Корпоративна система; и в) да придобива точно копие на което и да е Устройство. Ако Kyndryl се нуждае от съдействието на Доставчика, за да упражни правата си, Доставчикът изпълнява изцяло и в срок исканията на Kyndryl за подобно съдействие (включително например искане за сигурно конфигуриране на което и да е Устройство, инсталиране на софтуер за мониторинг или друг софтуер на което и да е Устройство, споделяне на подробности за връзка на системно ниво, ангажиране при мерки за реакция на инциденти за което и да е Устройство и осигуряване на физически достъп на Kyndryl до което и да е устройство за получаване на точно копие или с друга цел, както и други подобни и свързани искания).

3.2 Kyndryl има право да отмени достъпа до Корпоративните системи по всяко време, за който и да е служител на Доставчика или за всички служители на Доставчика, без предварително да уведомява Доставчика, служител на Доставчика или други лица, ако Kyndryl смята, че това е необходимо, за да се защити Kyndryl.

3.3 Правата на Kyndryl не се блокират, намаляват или ограничават по какъвто и да е начин от която и да е разпоредба на Документа по сделката, свързания основен договор или друг договор между страните, включително която и да е разпоредба, която изисква данни, материали или друга информация от какъвто и да е вид да се съхраняват само на определено място или места или изисква само лица от избрано място или места да имат достъп до тези данни, материали или друга информация.

4. Устройства на Kyndryl

4.1 Kyndryl си запазва правото на собственост върху всички Устройства на Kyndryl, като Доставчикът носи отговорност за загуба на Устройствата, включително поради кражба, вандализъм или небрежност. Доставчикът няма да извършва или да разрешава промени в Устройства на Kyndryl без предварително писмено съгласие на Kyndryl, като под промяна се има

предвид всяка промяна в софтуер, приложения, дизайн на сигурността, конфигурация на сигурността или физически, механичен или електрически дизайн.

4.2 Доставчикът връща всички Устройства на Kyndryl в рамките на 5 работни дни след приключване на необходимостта тези Устройства да предоставят Услугите и ако Kyndryl поиска, унищожава едновременно с това всички данни, материали и друга информация от всякакъв вид на тези Устройства, без да запазва копие, като следва Най-добрите индустриални практики, за да изтрие трайно всички данни, материали и друга информация. Доставчикът опакова и връща за своя сметка Устройствата на Kyndryl в същото състояние, в което са предоставени на Доставчика, с изключение на нормалното износване, до място, посочено от Kyndryl. Неспазването от страна на Доставчика на което и да е задължение от този раздел 4.2 представлява съществено нарушение на Документа по сделката и свързания основен договор и друг свързан договор между страните, като се има предвид, че даден договор се счита за „свързан“, ако достъпът до която и да е Корпоративна система улеснява задачите или други дейности на Доставчика по смисъла на този договор.

4.3 Kyndryl осигурява поддръжка за Устройствата на Kyndryl (включително проверка на Устройството и превантивна и възстановителна поддръжка). Доставчикът незабавно уведомява Kyndryl при нужда от ремонт.

4.4 За софтуерни програми, които Kyndryl притежава или има право да отдава под лиценз, Kyndryl предоставя на Доставчика временно право да използва, съхранява и прави достатъчно копия, за да поддържа разрешеното използване на Устройствата на Kyndryl. Доставчикът няма право да прехвърля програми на когото и да било, да прави копия на информацията за софтуерния лиценз, нито да разглобява, декомпилира, да конструира обратно или по друг начин да преобразува каквато и да е програма, освен ако това не е изрично разрешено от приложимото законодателство, без възможност за отказ от отговорност по договора.

5. Актуализиране

5.1 Независимо от разпоредби с противоположен смисъл в Документа по сделката или свързания основен договор между страните, след писмено известие до Доставчика и без да е необходимо съгласието на Доставчика, Kyndryl може да актуализира, допълва или по друг начин да изменя този Член, за да отговори на всяко изискване на приложимото законодателство или задължение на Клиента, за да отразява всяко допълнение към най-добрите практики за сигурност или по друг начин, както Kyndryl смята за необходим във връзка със защитата на Корпоративните системи или Kyndryl.

Член VII, Увеличаване на персонала

Този Член важи, когато служителите на Доставчика отделят цялото си работно време за предоставяне на Услуги за Kyndryl, извършват всички тези услуги в обекти на Kyndryl, обекти на Клиента или от домовете си, и предоставят Услуги, само като използват Устройства на Kyndryl за достъп до Корпоративните системи.

1. Достъп до Корпоративни системи; Среди на Kyndryl

1.1 Доставчикът има право да изпълнява Услугите, като осъществява достъп до Корпоративните системи само през Устройства, предоставени от Kyndryl.

1.2 Доставчикът спазва Условията, изложени в Член VI (Достъп до корпоративни системи), във връзка с какъвто и да е достъп до Корпоративните системи.

1.3 Устройствата, предоставени от Kyndryl, са единствените Устройства, които Доставчикът и неговите служители могат да използват за предоставяне на Услуги, като тези Устройства могат да бъдат използвани от Доставчика и неговите служители само за предоставяне на Услугите. За повече яснота, Доставчикът или неговите служители в никакъв случай нямат право да използват други устройства, за да предоставят Услуги, или да използват Устройства на Kyndryl за който и да е друг клиент на Доставчика или за каквато и да е друга цел освен за предоставяне на Услугите на Kyndryl.

1.4 Служителите на Доставчика, използващи Устройства на Kyndryl, могат да споделят Материали на Kyndryl помежду си и да съхраняват такива материали на Устройства на Kyndryl, но само до степен, в която такова споделяне и съхранение е необходимо за успешното изпълнение на Услуги.

1.5 Освен за целите на подобно съхранение на Устройства на Kyndryl, Доставчикът или неговите служители в никакъв случай нямат право да премахват Материали на Kyndryl от хранилища, среди, инструменти или инфраструктура на Kyndryl, където те се съхраняват от Kyndryl.

1.6 За повече яснота, Доставчикът и неговите служители нямат право да прехвърлят никакви Материали на Kyndryl в каквито и да са хранилища, среди, инструменти или инфраструктура на Доставчика или други системи, платформи, мрежи или други подобни структури на Доставчика без предварителното писмено съгласие на Kyndryl.

1.7 Член VIII (Технически и организационни мерки, Обща сигурност) не важи за Услугите на Доставчика, когато служителите на Доставчика отделят цялото си работно време за предоставяне на Услуги за Kyndryl, извършват всички тези услуги в обекти на Kyndryl, обекти на Клиента или от домовете си и предоставят Услуги, само като използват Устройства на Kyndryl за достъп до Корпоративните системи. Във всички останали случаи Член VIII важи за Услугите на Доставчика.

Член VIII, Технически и организационни мерки, Обща сигурност

Настоящият Член е приложим ако Доставчикът предоставя Услуги или Продукти на Kyndryl, освен когато Доставчикът ще има достъп само до ИСК на Kyndryl при предоставянето на тези Услуги или Продукти (т.е. Доставчикът няма да Обработва други Данни на Kyndryl, или да има достъп до други Материали на Kyndryl, или до Корпоративна система), единствените Услуги и Продукти на Доставчика са да предостави на Kyndryl Софтуер на място или Доставчикът предоставя всички свои Услуги и Продукти чрез модел на увеличаване на персонала съгласно Член VII, включително Раздел 1.7 от него.

Доставчикът спазва изискванията на този Член и по този начин защитава: а) Материали на Kyndryl срещу загуба, унищожаване, изменение, случайно или неразрешено разкриване и случаен или неразрешен достъп; б) Данни на Kyndryl от незаконни начини на Обработване; и в) Технологии на Kyndryl от незаконни форми на Боравене. Изискванията на този Член се отнасят за всички ИТ приложения, платформи и инфраструктура, които Доставчикът използва или управлява при предоставянето на Продукти и Услуги и при Боравенето с Технологии на Kyndryl, включително всички разработки, тествания, хостинг, поддръжка, операции и среди на центровете за данни.

1. Политики за сигурност

1.1. Доставчикът поддържа и следва политиките и практиките за ИТ сигурност, които са неразделна част от бизнеса на Доставчика, задължителни за целия Персонал на Доставчика и съответстват на Най-добрите индустриални практики.

1.2. Доставчикът преразглежда своите политики и практики в областта на ИТ сигурността поне веднъж годишно и ги изменя, ако сметне за необходимо, за да защити Материалите на Kyndryl.

1.3. Доставчикът поддържа и следва стандартните, задължителни изисквания за проверка във връзка с наемането на нови служители и налага тези изисквания на целия Персонал на Доставчика и всички изцяло притежавани дъщерни дружества на Доставчика. Тези изисквания включват криминални проверки до степента, допустима от местните закони, доказателство за потвърждаване на самоличността и допълнителни проверки, които Доставчикът счита за необходими. Доставчикът периодично повтаря или препотвърждава тези изисквания, когато сметне за необходимо.

1.4. Доставчикът организира ежегодно обучение за сигурност и поверителност за своите служители и изисква всички тези служители всяка година да удостоверяват, че спазват етичните норми за бизнес поведение, правилата на поверителност и политиките за сигурност на Доставчика, както е посочено в кодекса за поведение на Доставчика или други подобни документи. Доставчикът провежда допълнително обучение по политики и процеси на лица с административен достъп до каквито и да са компоненти на Услуги, Продукти или Материали на Kyndryl, като такова обучение е специфично за тяхната длъжност и участие в Услугите, Продуктите и Материалите на Kyndryl, и е необходимо за поддържане на исканото съответствие и сертификати.

1.5. Доставчикът разработва мерки за сигурност и поверителност, за да защити и поддържа наличността на Материали на Kyndryl, включително чрез тяхното внедряване, поддръжка и съответствие с политики и процедури, изискващи сигурност и поверителност чрез проектиране, инженеринг на сигурността и сигурни операции за всички Услуги и Продукти и за всеки случай на Боравене с Технологии на Kyndryl.

2. Инциденти, свързани със сигурността

2.1. Доставчикът поддържа и спазва документирани политики за реагиране на инциденти, съответстващи на Най-добрите индустриални практики за справяне с инциденти, касаещи компютърната сигурност.

2.2. Доставчикът разследва неразрешения достъп или неразрешената употреба на Материали на Kyndryl и определя и изпълнява подходящ план за реагиране.

2.3. Доставчикът уведомява Kyndryl незабавно (и в никакъв случай не по-късно от 48 часа), след като установи Нарушение в сигурността. Доставчикът ще извършва това уведомяване чрез Портала на Kyndryl за глобално съдействие за доставките на https://www.kyndryl.com/procurement/procSupport. Доставчикът предоставя на Kyndryl основателно поискана информация за подобно нарушение и за състоянието на всички мерки, предприети от Доставчика по отстраняване и възстановяване. Тази основателно поискана

информация може да включва например регистрационни файлове, съдържащи данни за привилегирован, административен и друг достъп до Устройства, системи или приложения, точни копия на Устройства, системи или приложения и други подобни елементи до степента, отнасяща се до нарушението или до дейностите на Доставчика по отстраняване и възстановяване.

2.4. Доставчикът предоставя на Kyndryl разумно съдействие за изпълнението на каквито и да е правни задължения (включително задължения за уведомяване на регулаторните органи или Субектите на данните) на Kyndryl, свързани лица с Kyndryl и Клиенти (и техните клиенти и свързани лица) във връзка с Нарушение на сигурността.

2.5. Доставчикът няма да информира или уведомява трети страни, че Нарушение на сигурността, пряко или косвено е свързано с Kyndryl или Материали на Kyndryl, освен ако Kyndryl не разреши писмено това да бъде направено или ако това се изисква по закон. Доставчикът писмено ще информира Kyndryl преди да направи изисквано по закон уведомление до трета страна, ако уведомлението ще идентифицира Kyndryl, пряко или косвено.

2.6. В случай на Нарушение на сигурността, произтичаща от нарушение на Доставчика на което и да е от задълженията по тези Условия:

(a) Доставчикът поема всички разходи, които прави, както и действителните разходи, които Kyndryl прави, като уведомява действащите регулаторни органи, други правителствени и съответни индустриални саморегулаторни агенции, медиите (ако се изисква от приложимото законодателство), Субектите на данни, Клиенти и други;

(b) при поискване от Kyndryl Доставчикът създава и поддържа за своя собствена сметка кол център за отговори на въпроси от Субекти на данни относно Нарушения на сигурността и последствията от тях в продължение на 1 година след датата, на която съответните Субекти на данни са били уведомени за Нарушение на сигурността или както се изисква от приложимите закони за защита на данните, което от двете осигурява по-висока степен на защита. Kyndryl и Доставчикът работят заедно за създаване на сценарии и други материали, които да се използват от служителите в кол центъра при отговор на запитвания. Алтернативно, при писмено известие до Доставчика Kyndryl може да създаде и поддържа свой собствен кол център вместо Доставчика, а Доставчикът да възстанови на Kyndryl действителните разходи на Kyndryl за създаването и поддържането на такъв кол център; и

(c) Доставчикът възстановява на Kyndryl действителните разходи, които Kyndryl прави при предоставяне на услуги за мониторинг на кредити и възстановяване на кредити, в продължение на 1 година след датата, на която физическите лица, засегнати от нарушението, които избират да се регистрират за такива услуги, са били уведомени за Нарушението на сигурността, или съгласно изискванията на приложимите закони за защита на данните, което от двете осигурява по-голяма защита.

3. Физическа сигурност и Контрол на достъп (терминът „Обект“, използван по-долу, означава физическо местоположение, на което Доставчикът хоства, обработва или осъществява достъп до Материали на Kyndryl).

3.1. Доставчикът поддържа необходимия физически контрол на достъпа, например бариери, контролирани с карти входни пунктове, камери за наблюдение и обслужвани от служители приемни, за да се предпази от неправомерно влизане в Обектите.

3.2. Доставчикът изисква разрешение за достъп до Обекти и контролирани зони в рамките на Обектите, включително при временен достъп, и ограничава достъпа според длъжността и служебните задължения. Ако Доставчикът предостави временен достъп, негов упълномощен служител придружава всеки посетител, докато е на Обекта и в обхвата на контролираните зони.

3.3. Доставчикът въвежда физически контрол на достъпа, включително многофакторен контрол на достъпа в съответствие с Най-добрите индустриални практики, за да ограничи по подходящ начин влизането в контролираните зони на Обектите, регистрира всички опити за влизане и съхранява тези регистри най-малко за срок от една година.

3.4. Доставчикът отменя достъпа до Обекти и контролирани зони на Обекти в случай на а) освобождаване на упълномощен служител на Доставчика; или б) служебните задължения на упълномощения служител на Доставчика вече не изисква такъв достъп. Доставчикът спазва

стриктно официално въведените процедури за освобождаване, които включват незабавно премахване от списъците за контрол на достъпа и предаване на физическите пропуски за достъп.

3.5. Доставчикът предприеме предпазни мерки, за да защити цялата физическа инфраструктура, използвана за поддържане на Услугите и Продуктите и за Боравене с Технологии на Kyndryl, от заплахи за околната среда, както природни бедствия, така и причинени от човека, например прекалено висока температура на околната среда, пожар, наводнение, влажност, кражба и вандализъм.

4. Достъп, намеса, прехвърляне и контрол на разделянето

4.1. Доставчикът ще поддържа документирана архитектура на сигурността на мрежите, които управлява при своето изпълняване на Услугите, предоставяне на Продуктите и Боравене с Технологии на Kyndryl. Доставчикът отделно преглежда съответната мрежова архитектура и въвежда мерки за предотвратяване на неразрешени мрежови връзки към системи, приложения и мрежови устройства с цел спазване на стриктните стандарти за сигурно сегментиране, изолация и защита. Доставчикът няма право да използва безжична технология при своя хостинг и при опериране на каквито и да е Хоствани услуги; вместо това Доставчикът може да използва технология за безжична мрежа при предоставянето на Услуги и Продукти и при Боравенето с Технологии на Kyndryl, но при условие че шифрова и изисква сигурно удостоверяване за всякакви такива безжични мрежи.

4.2. Доставчикът поддържа мерки, които имат за цел да разделят логически и да предотвратяват излагането на Материали на Kyndryl на достъп от неупълномощени лица. Освен това Доставчикът поддържа подходяща изолация на своята производствена, непроизводствена и друга среда и ако Материали на Kyndryl вече присъстват или са прехвърлени в непроизводствена среда (например за възпроизвеждане на грешка), Доставчикът гарантира, че степента на защита и неприкосновеност в непроизводствената среда е еквивалентна на тези в производствената среда.

4.3. Доставчикът ще шифрова Материалите на Kyndryl в процес на транзит и в извън транзит (освен ако Доставчикът не докаже убедително за Kyndryl, че шифроването на Материалите на Kyndryl извън транзит не е осъществимо технически. Освен това Доставчикът шифрова всички физически носители, ако има такива, като например носители, съдържащи резервни копия на файлове. Доставчикът поддържа документирани процедури за генериране, издаване, разпространение, съхранение, ротация, отменяне, възстановяване, създаване на резервни копия, унищожаване, достъп и използване на ключове за сигурност, свързани с шифроване на данни. Доставчикът ще осигури всички специфични криптографски методи, използвани при такова шифроване, да отговарят на Най-добрите индустриални практики (като напр. NIST SP 800-131a).

4.4. Ако Доставчикът изисква достъп до Материали на Kyndryl, Доставчикът ограничава този достъп до най-ниското ниво, необходимо за предоставяне и поддържане на Услугите и Продуктите. Доставчикът изисква подобен достъп, включително административен достъп до каквито и да е основни компоненти (т.е. привилегирован достъп), да бъде индивидуален, базиран на длъжност и подлежащ на одобрение и редовна проверка от упълномощени служители на Доставчика съгласно принципите за разделение на задълженията. Доставчикът поддържа мерки за идентифициране и премахване на резервни или латентни акаунти. Доставчикът оттегля акаунти с привилегирован достъп в рамките на двадесет и четири (24) часа след освобождаване на собственика на акаунта или искането на Kyndryl или на упълномощен служител на Доставчика, като например мениджъра на собственика на акаунта.

4.5. В съответствие с Най-добрите индустриални практики, Доставчикът поддържа технически мерки, налагащи прекъсване на неактивни сесии, блокиране на акаунти след няколко последователни неуспешни опита за влизане, силни пароли или фраза за удостоверяване на достъп, както и мерки, изискващи сигурно прехвърляне и съхранение на тези пароли и фрази за достъп. Освен това Доставчикът използва многофакторно удостоверяване за всеки привилегирован достъп до Материали на Kyndryl, който не се осъществява от конзола.

4.6. Доставчикът следи използването на привилегирован достъп и поддържа информация за сигурност и мерки за управление на събития, предназначени за: а) идентифициране на

неразрешен достъп и дейност; б) улесняване на навременен и подходящ отговор на такъв достъп и дейност; и в) разрешаване на одити от Доставчика, Kyndryl (в съответствие с правата му за проверка, посочени в тези Условия, и правото на одит, посочени в Документа по сделката или свързан основен или друг договор между страните) и други лица за спазване на документираната политика на Доставчика.

4.7. Доставчикът съхранява регистрационните файлове, в които записва, в съответствие с Най-добрите индустриални практики, целия административен, потребителски или друг достъп или дейност до или по отношение на системите, използвани при предоставянето на Услуги или Продукти и при Боравенето с Технологии на Kyndryl (и предостави тези регистрационни файлове на Kyndryl при поискване). Доставчикът поддържа мерки, предназначени да защитават срещу неупълномощен достъп, изменение и случайно или преднамерено унищожаване на такива регистри.

4.8. Доставчикът поддържа компютърни защити за системи, които притежава или управлява, включително системи за крайни потребители, и които използва при предоставянето на Услуги или Продукти, или при Боравене с Технологии на Kyndryl, като такива защити могат да бъдат: защитни стени на крайната точка, шифроване на целия диск, технологии за откриване и реагиране, базирани на подпис или без подпис, за справяне със злонамерен софтуер и разширени устойчиви заплахи, базирано на време заключване на екрана и решения за управление на крайните точки, които налагат конфигуриране на сигурността и изисквания за коригиране. Освен това Доставчикът прилага технически и оперативни контролни мерки, които гарантират, че само познати и надеждни системи на крайни потребители имат разрешение да използват мрежите на Доставчика.

4.9. В съответствие с Най-добрите индустриални практики Доставчикът поддържа защити за среди на центровете за данни, където присъстват или се обработват Материали на Kyndryl, където тези защити включват установяване на проникване и превенция, както и противодействие и смекчаване на последиците при отказ на услугата.

5. Интегритет на услуги и системи и контрол на наличността

5.1. Доставчикът: а) извършва оценки на риска за сигурността и неприкосновеността на личните данни поне веднъж годишно; б) провежда тестове за сигурност и оценява уязвимостите, включително сканиране на сигурността на автоматизираната система и приложенията и ръчно етично хакване, преди пускане на продукцията и ежегодно след това, когато се отнася до Услугите и Продуктите, и ежегодно по отношение на Боравенето с Технологии на Kyndryl; в) ангажира квалифицирана независима трета страна, която да извършва тестване за проникване в съответствие с Най-добрите индустриални практики поне веднъж годишно, като тестовете могат да бъдат автоматизирани и ръчни; г) извършва автоматизирано управление и рутинна проверка на спазването на изискванията за конфигуриране на сигурността за всеки компонент на Услугите и Продуктите и по отношение на Боравенето с Технологии на Kyndryl; и д) отстранява установени уязвимости или несъответствие със своите изисквания за конфигуриране на сигурността въз основа на свързания риск, експлоатация и въздействие. Доставчикът предприема разумни стъпки, за да избегне прекъсването на Услугите при извършване на тестове, оценки, сканиране и изпълнение на дейности по възстановяване. По искане на Kyndryl Доставчикът предоставя на Kyndryl писмено резюме на последните тествания за проникване на Доставчика, което представлява доклад, съдържащ поне наименованието на офертите, обхванати от тестването, броя на системите или приложенията, включени в обхвата на тестването, датите на тестване, използваната методология и качествено обобщение на Продуктите.

5.2. Доставчикът поддържа политики и процедури, предназначени за управление на рисковете, свързани с добавяне на промени в Услугите или Продуктите или с Боравенето с Технологии на Kyndryl. Преди да въведе съответната промяна, включително за засегнати системи, мрежи и свързани компоненти, Доставчикът документира в регистрирана заявка за промяна: а) описание и причина за промяната; б) подробности и график за въвеждането; в) декларация за риска, касаеща въздействието върху Услугите и Продуктите, клиентите на Услугите или Материалите

на Kyndryl; г) очакваният резултат; д) план за обратни действия; е) одобрение от упълномощени служители на Доставчика.

5.3. Доставчикът поддържа опис на всички ИТ активи, които използва при извършване на Услуги, предоставяне на Продукти и Боравене с Технологии на Kyndryl. Доставчикът непрекъснато наблюдава и управлява състоянието (включително и капацитета) и наличието на съответните ИТ активи, Услуги, Продукти и Технологии на Kyndryl, включително основните компоненти на тези активи, Услуги, Продукти и Технологии на Kyndryl.

5.4. Доставчикът изгражда всички системи, които използва при разработването или извършването на Услугите и Продуктите и при Боравенето с Технологии на Kyndryl, от предварително дефинирани изображения на системи за сигурност или базови линии за сигурност, които отговарят на Най-добрите индустриални практики, например сравнителните показатели на Центъра за интернет сигурност (ЦИС).

5.5. Без да ограничава задълженията на Доставчика или правата на Kyndryl, посочени в Документа по сделката или свързания основен договор между страните по отношение на непрекъснатостта на бизнеса, Доставчикът оценява отделно всяка Услуга и Продукт и всяка ИТ система, използвана при Боравене с Технологии на Kyndryl за непрекъснатост на бизнеса и ИТ и спрямо изискванията за възстановяване при бедствия съгласно документираните указания за управление на риска. Доставчикът гарантира, че всяка такава Услуга, Продукт и ИТ система, до степента, предвидена в оценката на риска, дефинира, документира, поддържа и ежегодно утвърждава планове за непрекъснатост на бизнеса и ИТ и възстановяване при бедствия в съответствие с Най-добрите индустриални практики. Доставчикът гарантира, че тези планове са разработени така, че да се спазват конкретните срокове за възстановяване, посочени в Раздел 5.6 по-долу.

5.6. Конкретните целеви точки на възстановяване („**ЦТВ**“) и целеви срокове за възстановяване („**ЦСВ**“) с оглед на която и да е Хоствана услуга са: 24 часа ЦТВ и 24 часа ЦСВ; независимо от това Доставчикът спазва ЦТВ или ЦСВ с по-кратка продължителност, ако Kyndryl го е договорила с Клиента, и след като Kyndryl надлежно уведоми писмено Доставчика за по-малките ЦТВ или ЦСВ (имейлът се приема за писмено уведомление). Тъй като това касае всички други Услуги, предоставяни от Доставчика на Kyndryl, Доставчикът гарантира, че плановете му за непрекъснатост на бизнеса и възстановяване при бедствия са разработени така, че да гарантират ЦТВ и ЦСВ, които позволяват на Доставчика да поддържа съответствие за всички свои задължения към Kyndryl съгласно Документа по сделката и свързан основен договор между страните и настоящите Условия, включително неговите задължения за своевременно тестване, съдействие и поддръжка.

5.7. Доставчикът поддържа мерки, предназначени за оценяване, тестване и прилагане на препоръчителни корекции за сигурност във връзка с Услугите и Продуктите и свързани системи, мрежи, приложения и основни компоненти в обхвата на тези Услуги и Продукти, както и системите, мрежите, приложенията и основните компоненти, използвани за Боравене с Технологии на Kyndryl. Ако се установи, че дадена препоръчителна корекция за сигурност е приложима и подходяща, Доставчикът я прилага съгласно насоките за документирана оценка на сериозността и риска. Прилагането от страна на Доставчика на препоръчителни корекции за сигурност се урежда от неговата политика за управление на промени.

5.8. Ако Kyndryl има основание да смята, че хардуерът или софтуерът, който Доставчикът предоставя на Kyndryl, може да съдържа проникващи елементи, например шпиониращ софтуер, злонамерен софтуер или злонамерен код, то тогава Доставчикът си сътрудничи спешно с Kyndryl за проучване и отстраняване на притесненията на Kyndryl.

6. Предоставяне на услуги

6.1 Доставчикът ще поддържа обичайните в индустрията методи за интегрирано удостоверяване на акаунти на Kyndryl или Клиенти, като Доставчикът ще следва Най-добрите индустриални практики при удостоверяването на такива акаунти на Kyndryl или Клиенти (напр. чрез централно управлявано от Kyndryl многофакторно Единно вписване, използващо OpenID Connect или Security Assertion Markup Language).

7. **Подизпълнители.** Без да се ограничават задълженията на Доставчика или правата на Kyndryl по Документа по сделката или свързания основен договор между страните по отношение на ангажирането на подизпълнители, Доставчикът ще осигури всеки работещ за него подизпълнител, извършващ работа за Доставчика, да въведе мерки за контрол на управлението с цел изпълнение на изискванията и задълженията, които тези Условия налагат на Доставчика.
8. **Физически носители**. Доставчикът почиства по безопасен начин физическите носители, предназначени за повторна употреба, преди самата употреба и унищожава носители, които не са предназначени за повторна употреба, като се придържа към Най-добрите индустриални практики за почистване на физическите носители.

Член IX, Сертифициране и доклади за Хоствани услуги

Този Член е в сила, ако Доставчикът предлага Хоствана услуга на Kyndryl.

1.1 Доставчикът получава следните сертификати и доклади в сроковете, упоменати по-долу:

Сертификати/доклади	**Времева рамка**
По отношение на Хостваните услуги на Доставчика: Удостоверяване на съответствие с ISO 27001, Информационни технологии, техники за сигурност, системи за управление на информационната сигурност, като сертификатите са базирани на оценка от компетентен независим одитор **Или** SOC 2 Тип 2: Доклад от компетентен независим одитор, който демонстрира, че е извършил преглед на системите, контролите и операциите на Доставчика в съответствие със SOC 2 Тип 2 (включително най-малко за сигурност, поверителност и наличност)	Доставчикът получава сертифициране по ISO 27001 до 120 дни след влизане в сила на Документа по сделката* или на друга Дата на задължаване** и след това подновява сертифицирането въз основа на оценката на компетентен независим одитор на всеки 12 месеца (всяко подновяване е съобразено с последната актуална версия на стандарта) Доставчикът ще получи доклада съгласно SOC 2 Тип 2 до 240 дни след датата на влизане в сила на Документа по сделката* или Дата на задължаване**и след това ще получава нов доклад от компетентен независим одитор, който демонстрира, че е извършил преглед на системите, контролите и операциите на Доставчика в съответствие с SOC 2 Тип 2 (включително най-малко за сигурност, поверителност и наличност) на всеки 12 месеца след това * Ако към тази дата на влизане в сила Доставчикът предоставя Хоствана услуга ** Датата, на която Доставчикът поема задължение за предоставяне на Хоствана услуга

1.2 Ако Доставчикът заяви писмено, а Kyndryl одобри писмено, Доставчикът има право да получи по същество еквивалентно сертифициране или доклад за описаните по-горе елементи с разбирането, че сроковете, посочени в таблицата по-горе, се прилагат непроменени с оглед на принципно еквивалентно сертифициране или доклад.

1.3 Доставчикът: а) при поискване незабавно предоставя на Kyndryl копие от всеки сертификат и доклад, който Доставчикът е длъжен да получи; и б) незабавно отстранява всякакви пропуски във вътрешния контрол, отбелязани по време на SOC 2 или в други принципно еквивалентни (ако Kyndryl одобрява) прегледи.

Член X, Сътрудничество, проверка и възстановяване

Този Член е в сила, ако Доставчикът предоставя Услуги или Продукти на Kyndryl.

1. Съдействие на Доставчика

1.1. Ако Kyndryl има причина да се съмнява, че Услуги или Продукти може да са допринесли, допринасят или може да допринесат за проблем с киберсигурността, Доставчикът разумно съдейства при всяко запитване на Kyndryl относно такъв проблем, включително като своевременно и пълно отговаря на искания за информация, било чрез документи, други записи, интервюта със съответен Персонал на Доставчика и т.н.

1.2. Страните се договарят: а) да си предоставят взаимно при поискване такава допълнителна информация; б) да изготвят и да си предоставят взаимно необходимите други документи; и в) да извършват такива други действия и неща, които другата страна би поискала разумно с цел изпълнение на целта на тези Условия и съгласно документите, посочени в тези Условия. По искане на Kyndryl например Доставчикът предоставя в разумен срок условията за поверителност и защита, включени в негови писмени договори с Подобработващи, включително, когато Доставчикът има право да направи това, като предостави достъп до самите договори.

1.3. По искане на Kyndryl Доставчикът предоставя информация за държавите, в които неговите Продукти и компонентите на тези Продукти са произведени, разработени или по-друг начин постигнати.

2. Проверка (терминът „Обект“, използван по-долу, означава физическо местоположение, на което Доставчикът хоства, обработва или осъществява достъп до Материали на Kyndryl)

2.1. Доставчикът поддържа подлежащ на одит запис, демонстриращ съответствие с тези Условия.

2.2. Kyndryl, самостоятелно или чрез външен одитор, може след 30-дневно предварително писмено уведомление до Доставчика да провери съответствието на Доставчика с тези Условия, включително чрез достъп до който и да е Обект или Обекти за такива цели, въпреки че Kyndryl няма да осъществява достъп до който и да е център за данни, където Доставчикът Обработва Данни на Kyndryl, освен ако няма основателна причина да смята, че по този начин ще получи необходимата информация. Доставчикът съдейства на Kyndryl при извършване на проверката, включително чрез своевременна и ефективна реакция на исканията за информация, независимо дали чрез документи, други записи, интервюта на съответния Персонал на Доставчика или други. Доставчикът има право да предложи на вниманието на Kyndryl доказателство за спазване на одобрен кодекс за поведение или индустриален сертификат или по друг начин да удостовери, че поддържа съответствие с тези Условия.

2.3. Проверката няма да се извършва повече от веднъж на 12 месеца, освен ако: а) Kyndryl проверява как Доставчикът се е справил с отстраняването на проблемите, установени при проверката за предходния 12-месечен период или (б) е възникнало Нарушение на сигурността и Kyndryl желае да провери спазването на задължения, свързани с нарушението. И в двата случая Kyndryl предоставя 30-дневно предварително писмено известие, както е посочено в Раздел 2.2 по-горе, но спешността на отстраняването на Нарушение на сигурността може да наложи на Kyndryl да извърши проверка преди изтичане на 30-дневното писмено предизвестие.

2.4. Регулаторен орган или друг Администратор може да упражни същите права като тези на Kyndryl, посочени в Раздели 2.2 и 2.3, като се има предвид, че регулаторният орган може да упражнява всякакви допълнителни права, които има съгласно закона.

2.5. Ако Kyndryl има разумно основание да заключи, че Доставчикът не спазва никое от тези Условия (независимо дали това основание произтича от проверка съгласно тези Условия, или по друг начин), то в такъв случай Доставчикът отстранява незабавно установеното несъответствие.

3. Програма за борба с фалшифицирането

3.1. Ако Продуктите на Доставчика включват електронни компоненти (например твърди дискове, SSD дискове, памет, централни процесорни устройства, логически устройства или кабели), Доставчикът поддържа и следва документирана програма за предотвратяване на фалшифицирането, най-вече за да избегне предоставянето на фалшиви компоненти на Kyndryl и, след това за да открива и коригира своевременно всеки случай, в който Доставчикът погрешно предоставя фалшиви компоненти на Kyndryl. Доставчикът налага същото задължение за поддържане и следване на документирана програма за предотвратяване на фалшифицирането на всички свои доставчици, които предоставят електронни компоненти, включени в Продуктите на Доставчика за Kyndryl.

4. Отстраняване на щети

4.1. Ако Доставчикът не изпълни свое задължение по настоящите Условия и това неизпълнение доведе до Нарушение на сигурността, Доставчикът ще поправи неизпълнението и ще отстрани вредните последици на Нарушението на сигурността, като поправянето и отстраняването ще бъдат съгласно разумните указания и график, определени от Kyndryl. Ако все пак Нарушението на сигурността произтича от предоставяне от Доставчика на Хоствана услуга с много ползватели и като следствие засегне много клиенти на Доставчика, включително Kyndryl, тогава Доставчикът, съобразно естеството на Нарушението на сигурността, своевременно и подходящо ще коригира неизпълнението при предоставянето й и ще отстрани вредните последици от Нарушението на сигурността, отчитайки в нужната степен евентуалния принос на Kyndryl за корекцията и отстраняването.

4.2. Kyndryl ще има право да участва в отстраняването на всяко Нарушение на сигурността, упоменато в Раздел 4.1, както сметне за подходящо или необходимо, а Доставчикът ще поеме разходите и разноските си за отстраняване на неизпълнението от негова страна и разходите и разноските по отстраняването, които страните понесат във връзка с подобно Нарушение на сигурността.

4.3. Например разходите за отстраняване на щети и разходите, свързани с Нарушение на сигурността, биха могли да включват разходи за установяване и разследване на Нарушението на сигурността, определяне на отговорностите съгласно приложимите закони и разпоредби, предоставяне на известия за уязвимостта, осигуряване на кол центрове, услуги за мониторинг на кредити и възстановяване на кредити, презареждане на данни, коригиране на продуктови дефекти (включително чрез Първичен код или друга разработка), ангажиране на трети страни за съдействие за предходни или други свързани дейности, както и други разходи, необходими за отстраняване на вредните последици от Нарушението на сигурността.За яснота, разходите и разноските по отстраняване не включват пропуснати от Kyndryl печалби, поръчки, стойност, приходи, клиентела или очаквани икономии.