Член I, Информация за бизнес контакт

Този Член се прилага, ако Доставчикът или Kyndryl обработва ИБК на другата страна

1.1 Kyndryl и Доставчикът могат да обработват ИБК на другата страна, когато извършват дейности във връзка с доставката на Услуги и Продукти от Доставчика.

1.2 Всяка страна:

(a) няма да използва или разкрива ИБК на другата страна за каквато и да е друга цел (за яснота никоя от страните няма да Продава ИБК на другия или използва или разкрива ИБК на другия за каквато и да е маркетингова цел без предварителното писмено съгласие на другата страна и, когато е необходимо, предварителното писмено съгласие на засегнатите Субекти на данни), и

(b) ще изтрие, модифицира, коригира, върне, предостави информация относно обработката, ограничи обработката или предприеме всяко друго разумно заявено действие по отношение на ИБК на другия незабавно по писмено искане на другата страна, когато възникне неоторизирано използване на лична информация и страната иска да спре обработката и да отстрани нередностите.

1.3 Страните не влизат във взаимоотношения на съвместен администратор по отношение на ИБК на другата страна и никаква разпоредба на Документа по сделката няма да се тълкува или счита като указание за каквито и да било намерения за установяване на взаимоотношения на съвместен администратор.

1.4 Декларацията за поверителност на Kyndryl на адрес https://www.kyndryl.com/us/en/privacyсъдържа допълнителни подробности за обработката на ИБК от Kyndryl.

1.5 Страните са въвели и ще поддържат технически и организационни мерки за сигурност с цел защита на ИБК на другата страна срещу загуба, унищожаване, промяна, случайно или неоторизирано разкриване на данни, случаен или неоторизиран достъп и незаконна Обработка.

1.6 Доставчикът незабавно (и в никакъв случай по-късно от 48 часа) ще уведоми Kyndryl, ако установи нарушение на сигурността, включващо ИБК на Kyndryl. Доставчикът ще предостави такова известие до cyber.incidents@kyndryl.com. Доставчикът ще предостави на Kyndryl обосновано заявена информация относно такова нарушение, както и състоянието на всички дейности по отстраняването и възстановяването от страна на Доставчика. Обосновано заявената информация може да включва например регистрационни файлове, изразяващи привилегирован, административен и друг достъп до Устройства, системи или приложения, идентично копие (forensic images) на Устройства, системи или приложения и други подобни елементи, доколкото те са от значение във връзка с нарушението или дейностите по отстраняването и възстановяването от страна на Доставчика.

1.7 Когато Доставчикът обработва само ИБК на Kyndryl и няма достъп до никакви други данни или материали от какъвто и да е вид или до която и да е Корпоративна система на Kyndryl, настоящият Член и Член X (Сътрудничество, Проверка и Коригиране) са единствените Членове, които се прилагат към такава Обработка.

Член II, Технически и организационни мерки, Сигурност на Личните данни

Този Член се прилага, ако Доставчикът обработва данни на Kyndryl, различни от ИБК на Kyndryl. Доставчикът ще спазва изискванията на настоящия Член при предоставянето на всички Услуги и Продукти и по този начин защитава Личните данни на Kyndryl срещу загуба, унищожаване, промяна, случайно или неоторизирано разкриване на данни, случаен или неоторизиран достъп и незаконни видове на Обработка. Изискванията по настоящия Член се прилагат към всички IT приложения, платформи и инфраструктура, които Доставчикът експлоатира или управлява при предоставянето на Продукти и Услуги, включително всяко разработване, тестване, хостинг, поддръжка, дейности, които са планирани за постигане на определена цел и средите на центровете за данни.

1. Употреба на данни

1.1 Доставчикът няма право да добавя към Данните на Kyndryl или да включва с Данните на Kyndryl каквато и да е друга информация или данни, включително каквито и да е Лични данни, без предварителното писмено съгласие на Kyndryl и Доставчикът няма право да използва Данните на Kyndryl в обобщен или какъвто и да е друг вид, за каквато и да е цел различна от предоставянето на Услуги и Продукти (например, на Доставчика не е разрешено да използва или използва повторно Данни на Kyndryl за оценка на ефективността или като средства за подобряване на офертите на Доставчика, за изследователска и развойна дейност, за да създава нови оферти или да генерира отчети относно оферти на Доставчика). Освен ако не е изрично разрешено в Документа по сделката, на Доставчика е забранено да продава данни на Kyndryl.

1.2 На Доставчика се забранява да вгражда никакви технологии за уеб проследяване в Продуктите или като част от Услугите (такива технологии включвам HTML5, локално съхранение, етикети или маркери на трети страни и уеб маяци), освен ако не е изрично разрешено в Документа по сделката.

2. Искания на трети страни и Поверителност

2.1 Доставчикът няма да разкрива данни на Kyndryl на трета страна, освен ако не е оторизиран предварително от Kyndryl в писмен вид. Ако правителство, включително който и да е регулатор, изисква достъп до Данни на Kyndryl (напр. ако правителството на САЩ връчва заповед за национална сигурност на Доставчика, за да получи Данни на Kyndryl), или ако разкриване на данни на Kyndryl на друг се изисква по закон, Доставчикът ще уведоми Kyndryl писмено за такова искане или изискване и ще предостави на Kyndryl разумна възможност да оспори всяко разкриване на данни (когато законът забранява известяване, Доставчикът ще предприеме стъпки, които основателно смята за подходящи, за да оспори забраната и разкриване на данни на Kyndryl чрез съдебно действие или други средства).

2.2 Доставчикът уверява Kyndryl, че: (a) само тези негови служители, които се нуждаят от достъп до Данните на Kyndryl, за да предоставят Услуги или Продукти, ще имат такъв достъп, и то само до степента, необходима за предоставяне на тези Услуги и Продукти; и (b) е задължил служителите си за спазват поверителност, която изисква тези служители да използват и разкриват данните на Kyndryl само доколкото настоящите Условия позволяват.

3. **Връщане или Изтриване на данни на Kyndryl**

3.1 Доставчикът, по избор на Kyndryl, или ще изтрие, или ще върне Данните на Kyndryl при прекратяване или изтичане на Документа по сделката, или по-рано по искане на Kyndryl. Ако Kyndryl изисква изтриване, тогава Доставчикът, в съответствие с най-добрите практики в бранша, ще направи данните нечетими, така че да не бъдат повторно сглобени или реконструирани и ще удостовери изтриването на Kyndryl. Ако Kyndryl изисква връщане на Данните на Kyndryl, тогава Доставчикът ще направи това в разумния за Kyndryl срок и съгласно разумните писмени инструкции на Kyndryl.

Член III, Поверителност

Този Член се прилага, ако Доставчикът обработва Лични данни на Kyndryl.

1. Обработка

1.1 Kyndryl назначава Доставчика като Обработващ лични данни, за да обработва Лични данни на Kyndryl с единствената цел да предостави Продукти и Услуги в съответствие с инструкциите на Kyndryl, включително съдържащите се в настоящите Условия, Документа по сделката и свързания базов договор между страните. Ако Доставчикът не приеме инструкция, Kyndryl може да прекрати засегнатата част от Услугите чрез писмено предизвестие. Ако Доставчикът смята, че дадена инструкция нарушава закон за защита на данните, Доставчикът ще информира Kyndryl незабавно и в рамките на срока, изискван по закон. Ако Доставчикът не спази някое от задълженията си по настоящите Условия и това неспазване причини неоторизирано използване на Лична информация, или, общо казано, във всеки случай на неупълномощено използване на Лична информация, Kyndryl ще има право да спре обработката, да коригира неспазването и да отстрани вредните последици от неоторизираното използване, като това изпълнение и отстраняване се извършва по разумни указания и график на Kyndryl.

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

1.3 В Приложение към Документа по сделката или в самия Документ по сделката се посочва следното по отношение на данните на Kyndryl:

(a) Категории субекти на данни;
(b) видове Лични данни на Kyndryl;
(c) действия с данни и дейности по Обработка;
(d) времетраене и честота на Обработка; и
(e) списък на Подизпълнители, обработващи лични данни.

2. Технически и организационни мерки

2.1 Доставчикът ще прилага и поддържа техническите и организационни мерки, зададени в Член II (Технически и организационни мерки, Сигурност на данните) и Член VIII (Технически и организационни мерки, Обща сигурност), като по този начин ще осигури ниво на защита, подходящо за риска, свързна с неговите Услуги и Продукти. Доставчикът потвърждава и разбира ограниченията в Член II, настоящия Член III и Член VIII и ще ги спазва.

3. Права на субекта на данни и искания

3.1 Доставчикът ще информира Kyndryl незабавно (по график, който позволява на Kyndryl и всички други Администратори да изпълняват задълженията си по закон) за всяка заявка от Субект на данни да упражни каквито и да е права на Субекта на данни (напр. коригиране, изтриване или блокиране на данни) по отношение на Личните данни на Kyndryl. Доставчикът може също незабавно да насочи към Kyndryl Субекта на данни, който прави такава заявка. Доставчикът няма да отговаря на никакви заявки от Субекти на данни, освен ако не се изисква от закона или не е инструктиран писмено от Kyndryl да го направи.

3.2 Ако Kyndryl е длъжен да предостави информация относно Лични данни на Kyndryl на други Администратори или други трети страни (напр. Субекти на данни или регулатори), Доставчикът ще съдейства на Kyndryl, като предостави информация и предприеме други разумни действия, които Kyndryl поиска, по график, който позволява на Kyndryl своевременно да отговори на такива Други администратори или трети страни.

4. Подизпълнители, обработващи Лични данни

4.1 Доставчикът ще предостави на Kyndryl предварително писмено известие, преди да добави нов Подизпълнител, обработващ Лични данни или да разшири обсега на Обработка от съществуващ Подизпълнител, като с това писмено известие идентифицира името на Подизпълнителя и опише новия или разширен обхват на Обработката. Kyndryl може да възрази на всеки такъв нов Подизпълнител или разширен обхват с основателни причини по всяко време и ако го направи, страните ще работят заедно добросъвестно, за да разгледат възражението на Kyndryl. В зависимост от правото на Kyndryl да възрази по всяко време, Доставчикът може да възложи на новия Подизпълнител или да разшири обхвата на Обработката на съществуващия Подизпълнител, ако Kyndryl не е повдигнал възражение в рамките на 30 дни от датата на писменото известие на Доставчика.

4.2 Доставчикът ще наложи задълженията за защита на данните, сигурност и сертифициране съгласно настоящите Условия на всеки одобрен Подизпълнител, преди Обработка на каквито и да било Данни на Kyndryl от страна на Подизпълнител. Доставчикът е изцяло отговорен пред Kyndryl за изпълнението на задълженията на всеки Подизпълнител.

5. Международно обработване на данни

Както се използва по-долу:

Адекватна държава означава държава, предоставяща адекватно ниво на защита на данните по отношение на съответното прехвърляне съгласно приложимите закони за защита на данните или решения на регулаторите.

Вносител на данни означава Обработващ лични данни или Подизпълнител, който не е установен в Адекватна държава.

Стандартни договорни клаузи на ЕС („СДК на ЕС“) означава Стандартните договорни клаузи на ЕС (Решение 2021/914 на Комисията) с приложени клаузи по желание, с изключение на опция 1 от клауза 9(a) и опция 2 от клауза 17, както е официално публикуван наhttps://commission.europa.eu/publications/standard-contractual-clauses-international-transfers_en

Сръбски стандартни договорни клаузи („Сръбски СДК“)означава сръбските стандартни договорни клаузи както е прието от „Сръбския комисар за Информация от обществено значение и Защита на личните данни“, публикуван на https://www.poverenik.rs/images/stories/dokumentacija-nova/podzakonski-akti/Klauzulelat.docx.

Стандартни договорни клаузи („**СДК**“) означава договорните клаузи, изисквани от приложимите закони за защита на данните за прехвърляне на лични данни към Обработващи субекти, които не са установени в Адекватни държави.

Допълнително споразумение за международно прехвърляне на данни на Обединеното кралство към Стандартните договорни клаузи на Комисията на ЕС („Допълнително споразумение за Обединеното кралство") означава Допълнителното споразумение за международно прехвърляне на данни на Обединеното кралство към Стандартните договорни клаузи на Комисията на ЕС, официално публикувано на https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/.

Швейцарско допълнение към стандартните договорни клаузи на Комисията на ЕС („Швейцарско допълнение") означава договорните клаузи към Стандартните договорни клаузи на Комисията на ЕС, които се прилагат в съответствие с решението на Швейцарския орган за защита на данните (**"FDPIC"**) и в съответствие с Швейцарския федерален закон за защита на данните (**"FADP"**).

5.1 Доставчикът няма да прехвърля или разкрива (включително чрез отдалечен достъп) каквито и да било Лични данни на Kyndryl през граница без предварителното писмено съгласие на Kyndryl. Ако Kyndryl предостави такова съгласие, страните ще си сътрудничат, за да осигурят съответствие с приложимите закони за защита на данните. Ако СДК са задължителни съгласно тези закони, Доставчикът незабавно ще сключи СДК по заявка на Kyndryl.

5.2 По отношение на СДК на ЕС:

(a) Ако Доставчикът не е установен в Адекватна държава: Доставчикът с настоящото сключва СДК на ЕС с Kyndryl като Вносител на данни и Доставчикът ще сключи писмени споразумения с всеки одобрен Подизпълнител съгласно клауза 9 от СДК на ЕС и ще предостави на Kyndryl копия от тези споразумения при заявка.

(i) Модул 1 от СДК на ЕС не се прилага, освен ако страните не са договорили друго в писмен вид.

(ii) Модул 2 от СДК на ЕС се прилага, когато Kyndryl е Администратор, а Модул 3 се прилага, когато Kyndryl е Обработващ лични данни. В съответствие с Клауза 13 от СДК на ЕС, когато се прилагат Модули 2 или 3 страните се съгласяват, че (1) СДК на ЕСще се управлява от закона на държавата членка на ЕС, където се намира компетентният надзорен орган и (2) всички спорове, произтичащи от СДК на ЕС, ще бъдат решавани в съдилищата на държавата членка на ЕС, където се намира компетентният надзорен орган. Ако такъв закон в (1) не допуска права като трето лице бенефициер, тогава СДК на ЕС се уреждат от закона на Холандия и всички спорове, произтичащи от СДК на ЕС съгласно (2), ще бъдат разрешавани от съда на Амстердам в Холандия.

(b) Ако и двете страни, Доставчикът и Kyndryl, са установени в Адекватна държава, Доставчикът ще действа като Износител на данни и ще сключи СДК на ЕС с всеки одобрен Подизпълнител в Неадекватна държава. Доставчикът ще изпълни необходимата Оценка на въздействието на прехвърлянето (ОВП) и ще извести Kyndryl без ненужно забавяне относно (1) необходимостта да се приложат допълнителни мерки и (2) приложените мерки. При заявка Доставчикът ще предостави на Kyndryl резултатите от ОВП и всяка информация, необходима на Kyndryl за разбиране и оценка на резултатите. В случай, че Kyndryl не е съгласен с резултатите от ОВП на Доставчиците или приложените допълнителни мерки, Kyndryl и Доставчикът ще работят заедно за намиране на изпълнимо решение. Kyndryl запазва правото си да преустановява или прекратява услуги на Доставчиците без обезщетение. За да се избегне съмнение, това не освобождава Подизпълнител на Доставчика от задължението да стане страна по СДК на ЕС с Kyndryl или неговите Клиенти, както е посочено в раздел 5.2 (d) по-долу.

(c) Ако Доставчикът е установен в Европейското икономическо пространство и Kyndryl е Администратор, който не е предмет на Общия регламент за защита на данните 2016/679, тогава се прилага Модул 4 от СДК на ЕС и Доставчикът с настоящото влиза в СДК на ЕС с Kyndryl в качеството на износител на данни. Ако се прилага Модул 4 от СДК на ЕС, страните се съгласяват,че СДК на ЕС се уреждат от закона на Холандия и всички спорове, произтичащи от СДК на ЕС, се разрешават от съда на Амстердам в Холандия.

(d) Ако Други Администратори, като например Клиенти или филиали, отправят заявка да станат страна по СДК на ЕС съгласно „клауза за свързване “ в Клауза 7, Доставчикът с настоящото се съгласява с всяка такава заявка.

(e) Техническите и Организационни мерки, необходими за изпълнение на Приложение II на СДК на ЕС, могат да бъдат намерени в тези Условия, самият Документ по сделката и свързаният базов договор между страните.

(f) В случай на противоречие между СДК на ЕС и настоящите Условия, СДК на ЕС ще имат предимство.

5.3 По отношение на Допълнителното(ите) споразумение(я) за Обединеното кралство:

(a) Ако Доставчикът не е установен в държава с адекватно ниво на защита: (i) с настоящото Доставчикът сключва с Kyndryl Допълнително(и) споразумение(я) за Обединеното кралство в качеството на Вносител на данни в допълнение на СДК на ЕС, определени по-горе (както е приложимо, в зависимост от обстоятелствата, при които се извършват дейностите по обработването); и (ii) Доставчикът ще сключи писмени споразумения с всеки одобрен Подизпълнител, обработващ данни, като при поискване ще предостави на Kyndryl копия от тези споразумения.

(b) Ако Доставчикът е установен в държава с адекватно ниво на защита, а Kyndryl е Администратор на данни, спрямо когото не се прилага Общият регламент относно защитата на данните на Обединеното кралство (включен в законодателството на Обединеното кралство съгласно Закона за Европейския съюз (оттегляне) от 2018 г.), тогава с настоящото Доставчикът сключва Допълнително(и) споразумение(я) за Обединеното кралство в качеството на Износител на данни с Kyndryl в допълнение на СДК на ЕС, определени в Раздел 5.2(б) по-горе.

(c) Ако други администратори на данни, като например Клиенти или филиали, поискат да станат страна по Допълнителното(ите) споразумение(я) за Обединеното кралство, Доставчикът се съгласява с всяко такова искане.

(d) Информацията в Приложението (както е определено в таблица 3) в Допълнителното(ите) споразумение(я) за Обединеното кралство може да бъде намерена в приложимите СДК на ЕС, в настоящите условия, в самия Документ по сделката и в свързания базов договор между страните. Нито Kyndryl, нито Доставчикът могат да прекратят Допълнителното(ите) споразумение(я) за Обединеното кралство, когато Допълнителното споразумение за Обединеното кралство се промени.

(e) В случай на каквото и да е противоречие между Допълнителното(ите) споразумение(я) за Обединеното кралство и настоящите Условия Допълнителното(ите) споразумение(я) за Обединеното кралство има(т) предимство.

5.4 Относно сръбските СДК:

(a) Ако Доставчикът не е установен в Адекватна държава: (i) Доставчикът с настоящото влиза в сръбските СДК с Kyndryl от името на Доставчика като Обработващ лични данни; и (ii) Доставчикът ще сключи писмени споразумения с всеки одобрен Подизпълнител, в съответствие с Член 8 от Сръбските СДК, и ще предостави на Kyndryl копия от тези споразумения при заявка.

(b) Ако Доставчикът е установен в Адекватна държава, тогава Доставчикът с настоящото сключва сръбски СДК с Kyndryl от името на всеки Подизпълнител, намиращ се в Неадекватна държава. Ако Доставчикът не е в състояние да направи това за който и да е Подизпълнител, тогава Доставчикът ще предостави на Kyndryl сръбските СДК, подписани от този Подизпълнител за насрещен подпис на Kyndryl, преди да позволи на Подизпълнителя да обработва Лични данни на Kyndryl.

(c) Сръбските СДК между Kyndryl и Доставчика ще служат или като сръбски СДК между Администратор и Обработващ лични данни, или като взаимно писмено споразумение между „обработващ лични данни“ и „подизпълнител обработващ лични данни“, в зависимост от

обстоятелствата. В случай на противоречие между сръбските СДК и настоящите Условия, сръбските СДК ще имат предимство.

(d) Информацията, необходима за изпълнение на Приложения от 1 до 8 от Сръбските СДК за целите на управлението на прехвърлянето на Лични данни към Неадекватна държава, може да бъде намерена в настоящите Условия и в Приложението към Документа по сделката или в самия Документ по сделката.

5.5. По отношение на швейцарското(ите) допълнение(я):

(a) Ако и доколкото прехвърлянето на Лични данни на Kyndryl съгласно раздел 5.1. е предмет на швейцарския Федерален закон за защита на данните („FADP") СДК на ЕС, договорени в раздел 5.2. от настоящите Условия се урежда прехвърлянето със следните изменения, за да се приеме стандартът на ОРЗД за швейцарските лични данни:

- Препратките към Общия регламент за защита на данните („ОРЗД") се разбират и като препратки към аналогични разпоредби на FADP,
- Швейцарската федерална информационна комисия за защита на данните е компетентният надзорен орган съгласно Клауза 13 и Приложение I.C от СДК на ЕС
- Швейцарското право като приложимо право, в случай че прехвърлянето е подчинено изключително на FADP, и
- Терминът„държава членка" в клауза 18 от СДК на ЕС се разширява, така че да включва Швейцария с цел да се даде възможност на швейцарските субекти на данни да упражняват правата си в мястото на обичайното си пребиваване.

(b) За да се избегне съмнение, нито едно от горепосочените действия няма за цел да намали по какъвто и да е начин нивото на защита на данните, осигурено от СДК на ЕС, а само да разшири това ниво на защита по отношение на швейцарските субекти на данни. Ако и доколкото това не е така, СДК на ЕС се ползва с предимство.

6. Съдействие и записи

6.1 Като се има предвид естеството на Обработката, Доставчикът ще съдейства на Kyndryl, като взема подходящи технически и организационни мерки за изпълнение на задълженията, свързани с исканията и правата на Субекта на данни. Доставчикът също така ще съдейства на Kyndryl за осигуряване на спазването на задълженията, свързани със защитата на Обработката, уведомяване и известяване при Нарушение на сигурността и изготвяне на оценки на въздействието върху защита на данните, включително предварителна консултация с отговорния регулатор, ако е необходимо, като се вземе под внимание информацията, достъпна на Доставчика.

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

Член IV, Технически и организационни мерки, Сигурност на кода

Настоящият Член се прилага, ако Доставчикът има достъп до Изходния код на Kyndryl. Доставчикът ще спазва изискванията на този Член и по този начин ще защити Изходния код на Kyndryl срещу загуба, разрушение, промяна, случайно или неоторизирано разкриване на данни, случаен или неоторизиран достъп и незаконни форми на боравене. Изискванията на настоящия Член се разширява към всички IT приложения, платформи и инфраструктура, които Доставчикът експлоатира или управлява при предоставянето на Продукти и Услуги, включително всяко разработване, тестване, хостинг, поддръжка, дейности, които са планирани за постигане на определена цел и средите на центровете за данни.

1. Изисквания за Защита

Както се използва по-долу:

Забранена държава означава всяка държава: (a) която правителството на САЩ е определило като чуждестранен противник съгласно Изпълнителната заповед от 15 май 2019 г. относно Защитата на веригата за доставки на информационни и комуникационни технологии и услуги, (b) включена в списъка в съответствие с раздел 1654 от Закона за националната отбрана на САЩ от 2019 г. или (c) идентифицирана като „Забранена държава“ в Документа по сделката.

1.1 Доставчикът няма да разпространява или поставя Изходен код на Kyndryl в доверителна сметка в полза на трета страна.

1.2 Доставчикът няма да позволи Изходен код на Kyndryl да се намира в сървъри, разположени в Забранена държава.Доставчикът няма да позволи на никого, включително на Персонала си, който се намира в Забранена държава или посещава Забранена държава (за обсега на всяко такова посещение), по каквато и да е причина, да осъществява достъп или използва Изходен код на Kyndryl, независимо къде по света се намира този Изходен код на Kyndryl и Доставчикът няма да позволи каквато и да е разработка, тестване или друга работа да се извършва в Забранена страна, които биха изисквали такъв достъп или ползване.

1.3 Доставчикът няма да поставя или разпространява Изходния код на Kyndryl в която и да е юрисдикция, където законът или тълкуването на закона изисква разкриване на Изходния код на трета страна. Ако има промяна на закон или тълкуване на закон в юрисдикция, където се намира Изходния код на Kyndryl, което може да доведе до задължение за Доставчика да разкрие такъв Изходен код на трета страна, Доставчикът незабавно ще унищожи или незабавно премахне такъв Изходен код на Kyndryl от такава юрисдикция, и няма да поставя никакъв допълнителен Изходен код в такава юрисдикция, ако такъв закон или тълкуване на закон остане в сила.

1.4 Доставчикът няма, пряко или косвено да предприеме каквото и да е действие , включително сключване на каквото и да е споразумение, което би накарало Доставчика, Kyndryl или трета страна да поеме задължение за разкриване на данни съгласно Раздели 1654 или 1655 от Закона за националната отбрана на САЩ от 2019 г. За по-голяма яснота, освен в случаите, когато това е изрично разрешено в Документа по сделката или свързания базов договор между страните, Доставчикът няма право да разкрива Изходен код на Kyndryl на която и да е трета страна, при никакви обстоятелства, без предварително писмено съгласие на Kyndryl.

1.5 Ако Kyndryl уведоми Доставчика или трета страна уведоми която и да е от страните, че: (a) Доставчикът е разрешил Изходния код на Kyndryl да бъде внесен в Забранена държава или друга юрисдикция, предмет на Раздел 1.3 по-горе, (b) Доставчикът в противен случай е направил достъпен, или е използвал Изходния код на Kyndryl по начин, непозволен от Документа по сделката или свързания базов договор, или друго споразумение между страните или (c) Доставчикът е нарушил Раздел 1.4 по-горе, тогава без да ограничава правата на Kyndryl за отстраняване на такова несъответствие по закон или по справедливост или според Документа по сделката или асоциирано базово или друго споразумение между страните: (i) ако такова известие е до Доставчика, тогава Доставчикът незабавно ще сподели за известието на Kyndryl; и (ii) Доставчикът, при разумна насока от Kyndryl, ще разследва и коригира проблема по график, който Kyndryl разумно определи (след консултация с Доставчика).

1.6 Ако Kyndryl основателно вярва, че промените в политиките, процедурите, контролите или практиките на Доставчика по отношение на достъпа до Изходния код може да са необходими за справяне с киберсигурността, кражба на интелектуална собственост или подобни или свързани рискове (включително риска, че без такива промени Kyndryl може да бъде ограничен да продава на определени Клиенти или на определени пазари или по друг начин не е в състояние да удовлетвори изискванията за защита на Клиента или верига за доставки), тогава Kyndryl може да се свърже с Доставчика, за да обсъди действията, необходими за справяне с такива рискове, включително промени в такива политики, процедури, контроли или практики. При заявка на Kyndryl, Доставчикът ще сътрудничи на Kyndryl при оценката на това дали такива промени са необходими и при прилагането на подходящи, взаимно договорени промени.

Член V, Сигурно разработване

Този Член се прилага ако Доставчикът ще предостави свой изходен код или изходен код на трета страна или локален софтуер на Kyndryl, или ако някои от Продуктите или Услугите на Доставчика ще бъдат предоставени на Клиент на Kyndryl като част от продукт или услуга на Kyndryl.

1. Готовност за Защита

1.1 Доставчикът ще си сътрудничи с вътрешните процеси на Kyndryl, които оценяват готовността за защита на продуктите и услугите на Kyndryl, които зависят от който и да е от Доставчиците, включително като отговаря на заявки за информация своевременно и изчерпателно, независимо дали това е чрез документи, други записи, интервюта със съответния Персонал на Доставчика или други подобни.

2. Сигурно разработване

2.1 Настоящият Раздел 2 се прилага само когато Доставчикът предоставя Локален софтуер на Kyndryl.

2.2 Доставчикът е въвел и ще поддържа през целия срок на Документа по сделката, в съответствие с най-добрите практики в бранша, политиката, процедурите и контролите за защита, насочени към мрежата, платформа, система, приложение, устройство, физическа инфраструктура, реакция при инциденти и персонала, необходими за защита на: (a) разработването, изграждането, тестването и операционните системи и среди, които Доставчикът или която и да е трета страна, ангажирана от Доставчика, експлоатира, управлява, използва или по друг начин разчита на или по отношение на Продуктите и (b) всички Продукти за изходен код срещу загуба, незаконни видове на боравене и неоторизиран достъп, разкриване на данни или промяна.

3. Сертифициране по ISO 20243

3.1 Настоящият Раздел 3 се прилага само ако някои от Продуктите или Услугите на Доставчика ще бъде предоставен на Клиент на Kyndryl като част от продукт или услуга на Kyndryl.

3.2 Доставчикът ще получи сертифициране 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). Като алтернатива, ако Доставчикът поиска писмено и Kyndryl одобри писмено, Доставчикът ще получи сертифициране за съответствие с еквивалентен по същество браншов стандарт, насочен към практиките на сигурно разработване и верига на доставки (или ертифициране чрез самооценка, или такъв, основан на оценката на компетентен независим одитор, ако и както Kyndryl одобри).

3.3 Доставчикът ще получи сертифициране за съответствие с ISO 20243 или еквивалентен по същество браншов стандарт (ако Kyndryl одобри писмено) до 180 дни след датата на влизане в сила на Документа по сделката
и след това подновява сертифицирането на всеки 12 месеца след това (с всяко подновяване спрямо тогавашната най- текуща версия на приложимия стандарт, т.е. ISO 20243 или, когато Kyndryl е одобрил писмено, еквивалентен по същество браншов стандарт, насочен към практиките на сигурно разработване и верига на доставки.

3.4 При подаване на заявка, Доставчикът незабавно ще предостави на Kyndryl копие от сертификатите, които Доставчикът е длъжен да получи, съгласно Раздели 2.1 и 2.2 по-горе.

4. Уязвимости в Защитата

Както се използва по-долу:

Поправка на грешка означава корекции на грешки и ревизии, които коригират грешки или недостатъци, включително Уязвимости в Защитата, на Продуктите.

Смекчаване означава всички известни средства за намаляване или избягване на рисковете от Уязвимост на Защитата.

Уязвимост на Защитата означава състояние в дизайна, кодирането, разработката, реализация, тестване, експлоатация, поддръжка, профилактика или управление на Продукт, което позволява атака от всеки, която може да доведе до неразрешен достъп или експлоатация, включително: (a) достъп до, контролиране или нарушаване на работата на системата, (b) достъп, изтриване, промяна или извличане на данни или (c) промени в идентичност, оторизации или разрешения на потребители или администратори. Уязвимостта на Защитата може да съществува независимо от това дали към нея е приписан идентификатор на Общи Уязвимости и Експозиции (ОУЕ) или някаква оценка или официална класификация.

4.1 Доставчикът декларира и гарантира, че ще: (a) използва най-добрите практики в бранша за идентифициране на уязвимости в сигурността, включително чрез непрекъснато статично и динамично сканиране на сигурността на приложения изходен код, сканиране на сигурността с отворен код и сканиране на системата на уязвимост, и (b) и спазва изискванията на настоящите Условия, за да спомогне за предотвратяване, засичане и коригиране на уязвимостите в сигурността в Продуктите и във всички IT приложения, платформи и инфраструктури, в и чрез които Доставчикът създава и предоставя Услуги и Продукти.

4.2 Ако Доставчикът узнае за Уязвимост на Защитата в Продукта или всяко такова IT приложение, платформа или инфраструктура, Доставчикът ще предостави на Kyndryl корекция на грешки и смекчаване за всички версии и издания на Продуктите в съответствие с нивата на сериозност и времеви рамки, определени в таблиците по-долу:

Ниво на сериозност*
Спешна Уязвимост на Защитата – това Уязвимост на Защитата, която представлява сериозна и потенциална глобална заплаха. Kyndryl определя Спешни уязвимости в Защитата по собствена преценка, независимо от основния резултат на Общата система за оценка на уязвимостта (ОСОУ).
Критичен – това е Уязвимост на Защитата, която има ОСОУ основен резултат от 9 до 10,0
Висок – това е Уязвимост на Защитата, която има ОСОУ основен резултат от 7,0 до 8,9
Среден – това е Уязвимост на Защитата, която има ОСОУ основен резултат от 4.0 до 6.9
Нисък – това е Уязвимост на Защитата, която има ОСОУ основен резултат от 0,0 до 3,9

Срокове

Спешен случай	***Критичен***	***Висок***	***Среден***	***Нисък***
4 дни или по-малко, както е определено от Главния офис за информационна сигурност на Kyndryl	30 дни	30 дни	90 дни	Според най-добрите практики в бранша

* Във всеки случай, където Уязвимостта на Защитата няма директно приписан основен резултат по ОСОУ, Доставчикът ще приложи Ниво на сериозност, което е подходящо за естеството и обстоятелствата на такава уязвимост.

4.3 За Уязвимост на Защитата, която е била публично разкрита и за която Доставчикът все още не е предоставил никаква корекция на грешка или смекчаване на Kyndryl, Доставчикът ще въведе всички технически осъществими допълнителни контроли за защита, които могат да смекчат рисковете от уязвимостта.

4.4 Ако Kyndryl не е доволен от реакцията на Доставчика спрямо която и да е Уязвимост на Защитата в даден Продукт или някое приложение, платформа или инфраструктура, споменати по-горе, тогава, без да се засягат други права на Kyndryl, Доставчикът незабавно ще уреди Kyndryl да обсъди опасенията си директно с Вицепрезидента на Доставчика или равностоен изпълнителен директор, който отговаря за доставката на Корекцията на грешки.

4.5 Примери за Уязвимости на Защитата включват код на трета страна или отворен код на край на експоатацията (КНЕ), където тези видове код вече не получават поправки за сигурност.

Член VI, Достъп до Корпоративни системи

Този Член се прилага, ако служителите на Доставчика ще имат достъп до която и да е Корпоративна система.

1. Общи условия

1.1 Kyndryl ще определи дали да оторизира служители на Доставчика за достъп до Корпоративните системи. Ако Kyndryl разреши това, тогава Доставчикът ще се съобрази и ще накара служителите си с такъв достъп да спазват изискванията на този Член.

1.2 Kyndryl ще идентифицира средствата, чрез които служителите на Доставчика могат да имат достъп до Корпоративни системи, включително дали тези служители ще осъществяват достъп до Корпоративни системи чрез Устройства предоставени от Kyndryl или Доставчика.

1.3 Служителите на Доставчика могат да имат достъп само до Корпоративни системи и могат да използват само Устройствата, които Kyndryl упълномощава за този достъп, за да предоставят Услуги. Служителите на Доставчика не могат да използват Устройствата, които Kyndryl разрешава, за да предоставят услуги на друго лице или субект, или за достъп до IT системи, мрежи, приложения, уеб сайтове, имейл средства, средства за сътрудничество или подобни или във връзка с Услугите на който и да е Доставчик или трета страна.

1.4 За яснота, служителите на Доставчика не могат да използват Устройствата, които Kyndryl разрешава за достъп до Корпоративни системи по каквато и да е лична причина (напр. Служителите на Доставчика не могат да съхраняват лични файлове като музика, видео клипове, снимки или други подобни атрибути на такива Устройства и не могат да използват Интернет от такива устройства по лични причини).

1.5 Служителите на Доставчика няма да копират Материали на Kyndryl, които са достъпни чрез Корпоративна система, без предварително писмено одобрение на Kyndryl (и никога няма да копират Материали на Kyndryl на преносимо устройство за съхранение, като USB, външно устройство с твърд диск или други подобни атрибути).

1.6 При заявка, Доставчикът ще потвърди, като назове името на служителя, специфичните Корпоративни системи, до които неговите служители имат оторизиран достъп, и са осъществявали достъп до тях, за произволен период от време, за който Kyndryl поиска данни.

1.7 Доставчикът ще уведоми Kyndryl в рамките на двадесет и четири (24) часа, след като всеки служител на Доставчика с достъп до която и да е Корпоративна система вече не е: (a) нает от Доставчика или (b) вече не работи по дейности, които изискват такъв достъп. Доставчикът ще работи с Kyndryl, за да гарантира, че достъпът за такива бивши или настоящи служители е незабавно отменен.

1.8 Доставчикът незабавно ще съобщи за всички действителни или подозирани инциденти на защитата (като загуба на Устройство на Kyndryl или на Доставчика или неоторизиран достъп до Устройство или данни, материали или друга информация от всякакъв вид) на Kyndryl и ще сътрудничи на Kyndryl при разследването на такива инциденти.

1.9 Доставчикът не може да разреши на който и да е агент, независим изпълнител или служител на подизпълнител да има достъп до Корпоративна система без предварителното писмено съгласие на Kyndryl; ако Kyndryl предостави това съгласие, тогава Доставчикът договорно ще ангажира тези лица и техните работодатели да спазват изискванията на този Член, все едно тези лица са служители на Доставчика, и ще носят отговорност пред Kyndryl за всички действия и бездействия от страна на всяко такова лице или работодател по отношение на такъв достъп до Корпоративна система.

2. Софтуер на Устройство

2.1 Доставчикът ще инструктира служителите си своевременно да инсталират на всички Устройства софтуер който Kyndryl изисква, за да се улесни достъпа до Корпоративните системи по защитен начин. Нито Доставчикът, нито неговите служители ще се намесват в дейности на този софтуер, или в защитните функции, които софтуера позволява.

2.2 Доставчикът и неговите служители ще се придържат към правилата за конфигурация на Устройството, които Kyndryl задава, и по друг начин ще работят с Kyndryl, за да гарантират, че софтуера функционира според намеренията на Kyndryl. Например Доставчикът няма да отменя софтуерното блокиране на уеб сайтове или автоматизирани функции за корекция.

2.3 Служителите на Доставчика нямат право да споделят Устройствата, които използват за достъп до Корпоративни системи, или техните потребителски имена на Устройството, пароли или други подобни, с друго лице.

2.4 Ако Kyndryl упълномощи служители на Доставчика да осъществяват достъп до Корпоративни системи с помощта на Устройства на Доставчика, тогава Доставчикът ще инсталира и стартира операционна система на тези устройства, които Kyndryl одобри, и ще въведе настройки за нова версия на тази операционна система или нова операционна система в разумен срок след като Kyndryl даде такива указания.

3. Надзор и Сътрудничество

3.1 Kyndryl има безусловното право да следи и коригира потенциални заплахи за проникване и други заплахи на киберсигурността по каквито и да е начини, от каквито и да е местоположения и използвайки каквито и да е средства, които Kyndryl смята за необходими или подходящи, без предварително известие към Доставчика или който и да е служител на Доставчика или други лица. Като примери за такива права, Kyndryl може, по всяко време, (a) да извърши тест за защита на всяко Устройство, (b) да следи, възстановява чрез технически или други средства и преглежда комуникации (включително имейл от всякакви акаунти за електронна поща), записи, файлове и други елементи, съхранявани във всяко Устройство или предадени чрез която и да е Корпоративна система, и (c) да придобива пълно изображение от електронната проверка на всяко Устройство. Ако Kyndryl се нуждае от сътрудничеството на Доставчика, за да упражни правата си, Доставчикът ще удовлетвори напълно и своевременно исканията на Kyndryl за такова сътрудничество (включително, например, искания за сигурно конфигуриране на всяко Устройство, инсталира следящ или друг софтуер на което и да е Устройство, споделя подробности за връзката на системно ново, ангажира в мерки за реакция при инцидент на всяко Устройство и осигурява физически достъп до всяко Устройство, така че Kyndryl да получи пълно изображение от електронната проверка или различно, и подобни и свързани заявки).

3.2 Kyndryl може да анулира достъпа до Корпоративните системи по всяко време, за всеки служител на Доставчик или за всички служители на Доставчик, без предварително известие на Доставчика или на който и да е служител на Доставчика или други, ако Kyndryl смята, че това е необходимо да се извърши за защита на Kyndryl.

3.3 Правата на Kyndryl не са блокирани, намалени или ограничени по какъвто и да е начин от каквато и да е разпоредба на Документа по сделката, свързания базов договор между страните или каквото и да е друго споразумение между страните, включително всяка разпоредба, която може да изисква данни, материали или друга информация от какъвто и да е вид да пребива само в избрано местоположение или местоположения, които могат да изискват само лица от избрано местоположение или местоположения да имат достъп до такива данни, материали или друга информация.

4. Устройства на Kyndryl

4.1 Kyndryl ще запази правото на собственост към всички Устройства на Kyndryl, като Доставчикът поема риска от загуба на Устройствата, включително поради кражба, вандализъм или небрежност. Доставчикът няма да прави или разрешава каквито и да било промени на Устройствата на Kyndryl без предварителното писмено съгласие на Kyndryl, като промяната включва всякаква промяна на Устройство, включително всяка промяна на софтуера на Устройството, приложения, дизайн на защитата, конфигурация на защитата или физически, механичен или електрически дизайн.

4.2 Доставчикът ще върне всички Устройства на Kyndryl в рамките на 5 бизнес дни, след като приключи необходимостта тези Устройства да предоставят Услуги, и ако Kyndryl поиска, унищожи всички данни, материали и друга информация от всякакъв вид на тези Устройства в същото време, без да запазва никакви копия като следва Най-добрите практики в бранша да изтрие напълно всички такива данни, материали и друга информация. Доставчикът ще опакова и върне Устройствата на Kyndryl в същото състояние, в което са били доставени на Доставчика, освен разумното износване, за негова сметка до местоположение, което Kyndryl посочи. Неспазването от страна на Доставчика на някое задължение в този Раздел 4.2 представлява съществено нарушение на Документа по сделката и свързания базов договор и на всяко свързано споразумение между страните, като се разбира, че споразумението е „свързано“, ако достъп до която и да е Корпоративна система улеснява задачите на Доставчика или други дейности по това споразумение.

4.3 Kyndryl ще осигури поддръжка за устройствата на Kyndryl (включително инспекция на Устройства и превантивна и коригираща профилактика). Доставчикът незабавно ще уведоми Kyndryl за необходимостта от коригираща услуга.

4.4. За софтуерни програми, които Kyndryl притежава или които има право да лицензира, Kyndryl предоставя на Доставчика временно право за ползване, съхраняване и да прави достатъчно копия, за да поддържа своето оторизирано ползване на Устройства на Kyndryl. Доставчикът няма право да прехвърля програми на никого, прави копия на информацията на софтуерния лиценз, или демонтира, декомпилира, извършва обратно инженерство или по друг начин превежда която и да е програма, освен ако не е изрично разрешено от приложимия закон без възможност за договорен отказ.

5. Актуализации

5.1 Независимо от каквото и да било в обратен смисъл в Документа по сделката или свързания базов договор между страните, при писмено известие до Доставчика и без необходимост да получи съгласието на Доставчика, Kyndryl може да обновява, допълва или изменя по друг начин този Член, за да разгледа всяко изискване съгласно приложимия закон или задължение на Клиента да отрази всяко развитие в най-добрите практики за защита или по друг начин, както Kyndryl смята за необходимо да защити Корпоративните системи или Kyndryl.

Член VII, Увеличаване на персонала

Този Член се прилага, когато служители на Доставчика ще отделят цялото си работно време за предоставяне на Услуги за Kyndryl, ще изпълняват всички тези Услуги в помещения на Kyndryl, помещения на Клиента или от домовете си и ще предоставят само Услуги използвайки Устройства на Kyndryl, за да получат достъп до Корпоративни системи.

1. Достъп до Корпоративни системи; Среди на Kyndryl

1.1 Доставчикът може да извършва Услуги само чрез достъп до Корпоративни системи, използвайки Устройства, които Kyndryl предоставя.

1.2 Доставчикът ще спазва условията указани в Член VI (Достъп до Корпоративни системи), за всякакъв достъп до Корпоративни системи.

1.3 Предоставените от Kyndryl Устройства са единствените Устройства, които Доставчикът и неговите служители могат да използват за предоставяне на Услуги и могат да се използват единствено от Доставчика и неговите служители за предоставяне на Услуги. За яснота, в никакъв случай Доставчикът или неговите служители не могат да използват други Устройства за предоставяне на Услуги или да използват Устройства на Kyndryl за друг клиент на Доставчика или за друга цел, различна от предоставяне на Услуги 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 Устройствата на Kyndryl, но само до ограничената степен, до която такова споделяне и съхранение е необходимо за успешното предоставяне на Услугите.

1.5 Освен по отношение на такова съхранение в Устройствата на Kyndryl, Доставчикът или неговите служители в никакъв случай не могат да преместват каквито и да е Материали на Kyndryl от хранилища, среди, средства или инфраструктура, където те се съхраняват от Kyndryl.

1.6 За яснота, Доставчикът и неговите служители не са оторизирани да прехвърлят каквито и да било Материали на Kyndryl до хранилища, среди, средства или инфраструктура на Доставчика, или други системи, платформи, мрежи или други подобни на Доставчика, без предварително писмено съгласие на Kyndryl.

1.7 Член VIII (Технически и Организационни мерки, Обща Сигурност) не се прилагат за Услугите на Доставчика, когато Служителите на Доставчика ще отделят цялото си работно време за предоставяне на Услуги за Kyndryl, ще изпълняват всички тези Услуги в помещения на Kyndryl, помещения на Клиента или от домовете си и ще предоставят само Услуги използвайки Устройства на Kyndryl, за да получат достъп до Корпоративни системи. В противен случай Член VIII се прилага за Услугите на Доставчика.

Член VIII, Технически и Организационни мерки, Обща Сигурност

Този Член се прилага, ако Доставчикът предоставя Услуги или Продукти на Kyndryl, освен ако Доставчикът ще има достъп само до ИБК на Kyndryl при предоставянето на тези Услуги и Продукти (т.е. Доставчикът няма да обработва други данни на Kyndryl или няма достъп до други материали на Kyndryl или до каквато и да е Корпоративна Система), единствените Услуги и Продукти на Доставчика са да предоставя локален софтуер на Kyndryl или Доставчикът предоставя всички свои Услуги и Продукти в модел за увеличаване на персонала съгласно Член VII, включително Раздел 1.7 от него.

Доставчикът ще спазва изискванията на този Член и по този начин защитава: (a) Материали на Kyndryl срещу загуба, разрушение, промяна, случайно или неразрешено разкриване и случаен или неразрешен достъп (b) незаконни форми на Обработка на данни на Kyndryl и (c) незаконни форми на боравене с Технологии на Kyndryl. Изискванията на настоящия Член се разширява към всички IT приложения, платформи и инфраструктура, които Доставчикът експлоатира или управлява при предоставянето на Продукти и Услуги, включително всяко разработване, тестване, хостинг, поддръжка, дейности, които са планирани за постигане на определена цел и средите на центровете за данни.

1. Политики за сигурност

1.1 Доставчикът ще поддържа и следва политиките и практиките за IT защита, които са неразделна част от бизнеса на Доставчика, задължителни за целия Персонал на Доставчика и в съответствие с най-добрите практики в бранша.

1.2 Доставчикът ще преглежда своите политики и практики за IT защита поне веднъж годишно и ще ги променя, както Доставчикът сметне за необходимо, за да защити Материалите на Kyndryl.

1.3 Доставчикът ще поддържа и следва стандартни изисквания за задължителна проверка при наемане на работа за всеки нает нов служител и ще разшири тези изисквания към всеки персонал на Доставчика и дъщерните дружества, изцяло притежавани от доставчика. Тези изисквания ще включват проверки на криминалното минало до степента, разрешена от местните закони, доказателство за удостоверяване на самоличността и допълнителни проверки, които Доставчикът счита за необходими. Доставчикът периодично ще повтаря и потвърждава валидността на тези изисквания, ако сметне за необходимо.

1.4 Доставчикът ще предоставя обучение по защита и конфиденциалност на служителите си ежегодно и ще изисква от всички такива служители да удостоверяват всяка година, че ще спазват политиките за етично бизнес поведение, поверителност и защита на Доставчика, както е изложено в кодекса на поведение на Доставчика или подобни документи. Доставчикът ще осигури допълнително обучение за политиката и процеса на лица с административен достъп до всякакви компоненти на Услугите, Продуктите или Материалите на Kyndryl, като такова обучение е специфично за тяхната роля и поддръжка на Услугите, Продуктите и Материалите на Kyndryl, и ако е необходимо за поддържане на изискваното съответствие и сертификати.

1.5 Доставчикът ще проектира мерки за защита и поверителност, за да защитава и поддържа свободното ползване на Материалите на Kyndryl, включително чрез неговото въвеждане, профилактика и съответствие с политики и процедури, които изискват защита и конфиденциалност чрез проектиране, защитно инженерство и защитни дейности за всички Услуги и Продукти и за всяко боравене с Технология на Kyndryl.

2. Инциденти със Защитата

2.1 Доставчикът ще поддържа и следва документирани политики за реакция при инцидент, отговарящи на най-добрите практики в бранша за управление на инциденти със защитата.

2.2 Доставчикът ще разследва неоторизиран достъп или неоторизирано използване на Материали на Kyndryl и ще определи и изпълни подходящ план за реакция.

2.3 Доставчикът незабавно (и при никакви обстоятелства по-късно от 48 часа) ще уведоми Kyndryl, ако установи нарушение на сигурността. Доставчикът ще предостави такова известие до cyber.incidents@kyndryl.com. Доставчикът ще предостави на Kyndryl обосновано заявена информация относно такова нарушение, както и състоянието на всички дейности по отстраняването и

възстановяването от страна на Доставчика. Обосновано заявената информация може да включва например регистрационни файлове, изразяващи привилегирован, административен и друг достъп до Устройства, системи или приложения, идентично копие (forensic images) на Устройства, системи или приложения и други подобни елементи, доколкото те са от значение във връзка с нарушението или дейностите по отстраняването и възстановяването от страна на Доставчика.

2.4 Доставчикът ще предостави на Kyndryl разумно съдействие за удовлетворяване на всички правни задължения (включително задължения да извести регулаторни органи или Субекти на данни) на Kyndryl, филиали на Kyndryl и Клиенти (и техните клиенти и филиали) във връзка с нарушение на защитата.

2.5 Доставчикът няма да информира или уведомява никоя трета страна, че нарушение на защитата е пряко или непряко свързано с Kyndryl или Материали на Kyndryl, освен ако Kyndryl не одобри това в писмен вид или когато се изисква по закон. Доставчикът ще уведоми Kyndryl в писмена форма преди да разпространи всяко законово изисквано известие на трета страна, когато известието би разкрило пряко или непряко идентичността на Kyndryl.

2.6 В случай на нарушаване на защитата, която произтича от нарушаване на задължение от Доставчика по настоящите Условия:

(a) Доставчикът ще бъде отговорен за всички разходи, които възникнат, както и за действителни разходи, които Kyndryl прави, при предоставяне на известие за нарушаване на защитата до приложими регулатори, други правителствени и съответните саморегулаторни агенции в бранша, медиите (ако се изисква от приложимия закон), Субекти на данни, Клиенти и други,

(b) ако Kyndryl поиска, Доставчикът ще създаде и поддържа за сметка на Доставчика кол-център, който да отговоря на въпроси от Субектите на данни относно нарушаване на защитата и последиците от това за 1 година след датата, на която тези Субекти на данни са били уведомени за нарушаване на защитата, или както се изисква от който и да е приложим закон за защита на данните, който от двете предоставя по-голяма защита. Kyndryl и Доставчикът ще работят заедно, за създаване сценарии и други материали, които да се използват от служителите на кол-центъра, когато отговарят на запитвания. Като алтернатива, при писмено заявление до Доставчика, Kyndryl може да създаде и поддържа свой собствен кол-център вместо да кара Доставчика да създаде кол-център, и Доставчикът ще възстанови на Kyndryl действителните разходи, които Kyndryl прави при създаването и поддържането на такъв кол-център, и

(c) Доставчикът ще възстанови на Kyndryl действителните разходи, които Kyndryl прави при предоставяне на услуги за кредитен мониторинг и кредитно възстановяване за 1 година след датата, на която лицата, засегнати от нарушаването, които избират да се регистрират за такива услуги, са били уведомени за нарушаване на защитата, или както се изисква от който и да е приложим закон за защита на данните, в зависимост от това кой от двете предоставя по-голяма защита.

3. Физическа Сигурност и контрол на Влизането (както се използва по-долу, „Обект“ означава физическо местоположение, където Доставчикът хоства, обработва или по друг начин има достъп до Материали на Kyndryl).

3.1 Доставчикът ще поддържа подходящи физически контроли за влизане, като например бариери, контролирани с карта точки за влизане, камери за наблюдение и рецепции с обслужващ персонал, за защита срещу неоторизирано влизане в Обектите.

3.2 Доставчикът ще изисква оторизирано одобрение за достъп до Обектите и контролираните зони в рамките на Обектите, включително всеки временен достъп, и ще ограничава достъпа според работните функции и бизнес нужди. Ако Доставчикът предостави временен достъп, неговият оторизиран служител ще придружава всеки посетител, докато е в Обекта и във всички контролирани зони.

3.3 Доставчикът ще въведе контроли за физически достъп, включително многофакторни системи за контрол на достъпа, които съответстват на най-добрите практики в бранша, за подходящо ограничаване

на влизането до контролираните зони в рамките на Обектите, ще записва всички опити за влизане и запазва такива регистри поне за една година.

3.4 Доставчикът ще анулиране достъпа до Обектите и контролираните зони в рамките на Обектите при (a) разделяне на оторизиран служител на Доставчика или (b) оторизираният служител на Доставчика вече няма валидна бизнес нужда от достъп. Доставчикът ще следва официални документирани процедури за разделяне, които включват бързо премахване от списъците за контролиран достъп и предаване на пропуски за физически достъп.

3.5 Доставчикът ще вземе предпазни мерки, за да защити всяка физическа инфраструктура, използвана за поддръжка на Услугите и Продуктите и Боравенето на Технология на Kyndryl срещу заплахи за средата както от естествено възникващи фактори, така от и такива, причинени от човека, като прекомерна температура на околната среда, пожар, наводнение, влажност, кражба и вандализъм.

4. Контрол на Достъпа, Намесата, Прехвърлянето и Разделянето

4.1 Доставчикът ще поддържа документирани мрежи на архитектура на сигурността, които управлява при функциониране на Услугите си, при осигуряване на Продуктите си и при Боравенето си с Технология на Kyndryl. Доставчикът ще преглежда отделно такава архитектурна мрежа и ще използва мерки за предотвратяване на неоторизирани мрежови връзки към системи, приложения и мрежови устройства, за съответствие със задълбочените стандарти за безопасно сегментиране, изолация и отбрана. Доставчикът не може да използва безжична технология в своя хостинг и дейности, на които и да е Хоствани Услуги; в противен случай Доставчикът може да използва безжична мрежова технология при доставката на Услуги и Продукти и при Боравене с Технология на Kyndryl, но Доставчикът ще шифрова и изисква защитна идентификация за всички такива безжични мрежи.

4.2 Доставчикът ще поддържа мерки, които са предназначени за логично отделяне и предотвратяване на Материалите на Kyndryl да бъдат изложени до или достъпни от неупълномощени лица. Освен това, Доставчикът ще поддържа подходяща изолация на своите производствени, непроизводствени и други среди, и ако Материалите на Kyndryl вече присъстват в или са прехвърлени към непроизводствени среди (например за възпроизвеждане на грешка), тогава Доставчикът ще гарантира, че защитите на сигурността и конфиденциалността в непроизводствената среда са равни на тези в производствената среда.

4.3 Доставчикът ще шифрова Материалите на Kyndryl по време на прехвърлянето и в покой (освен ако Доставчикът не докаже в задоволителна за Kyndryl степен, че шифроването на Материалите на Kyndryl в покой е технически неосъществимо). Доставчикът също ще шифрова всеки физически носител, ако има такъв, като например носител, съдържащ архивни файлове. Доставчикът ще поддържа документирани процедури за създаването на защитени ключове, издаване, разпределение, съхранение, ротация, отмяна, възстановяване, архивиране, унищожаване, достъп и използва криптиране по отношение на данни. Доставчикът ще гарантира, че специфичните криптографски методи, използвани за такова криптиране, се привеждат в съответствие с най-добрите практики в бранша (като например NIST SP 800-131a).

4.4 Ако Доставчикът изисква достъп до Материалите на Kyndryl, Доставчикът ще ограничи и стесни този достъп до най-ниското ниво, необходимо за предоставяне и поддържане на Услугите и Продуктите. Доставчикът ще изисква такъв достъп, включително административен достъп до всички основни компоненти (т.е. привилегирован достъп) било то индивидуален, според работните функции и ще подлежи на одобрение и редовно валидиране от оторизиран служители на Доставчика, в съответствие с принципите на разделяне на задълженията. Доставчикът ще поддържа мерки за идентифициране и премахване на излишни и неактивни акаунти. Доставчикът също ще анулира акаунти с привилегирован достъп в рамките на двадесет и четири (24) часа след като собственика на акаунта е бил освободен или при заявка от Kyndryl или който и да е оторизиран служител на Доставчика, като например мениджър на собственика на акаунта.

4.5 В съответствие с най-добрите практики в бранша, Доставчикът ще поддържа технически мерки, налагащи таймаут на неактивни сесии, блокиране на акаунти след многобройни последователни неуспешни опити за влизане, силна парола или фрази и мерки, изискващи сигурно прехвърляне и

съхранение на такива пароли и фрази. Освен това, Доставчикът ще използва многофакторно разпознаване за всеки неконзолен привилегирован достъп до всякакви Материали на Kyndryl.

4.6 Доставчикът ще наблюдава използването на привилегирован достъп и ще поддържа мерки за защита на информацията и мерки за управление на събитията, предназначени за: (a) идентифициране на неразрешен достъп и действия, (b) улесняване на навременна и подходяща реакция на такъв достъп и действия, и (c) разрешава одити от Доставчика, Kyndryl (съгласно своите права за проверка в настоящите Условия и права за одит в Документа по сделката или асоциирано базово или друго споразумение между страните) и други в съответствие с документираната политика на Доставчика.

4.7 Доставчикът ще задържа регистрационни файлове, в които записва, в съответствие с най-добрите практики в бранша, всеки административен, потребителски или друг достъп или действие към или по отношение на системите, използвани при предоставяне на Услуги или Продукти и при Боравене с Технологията на Kyndryl (и ще предостави тези регистрационни файлове на Kyndryl при заявка). Доставчикът ще поддържа мерки, предназначени за защита срещу неоторизиран достъп, модификация и случайно или умишлено разрушение на такива регистрационни файлове.

4.8 Доставчикът ще поддържа компютърни защити за системите, които притежава или управлява, включително системи за крайни потребители, и които използва при предоставяне на Услуги или Продукти или при Боравене с Технологията на Kyndryl, с такива защити, включително: защитна стена на крайна точка, пълно криптиране на диска, откриване на крайни точки със сигнатура и без сигнатура и технологии за реагиране за справяне със злонамерен софтуер и комплексни устойчиви заплахи, заключване на екрана според времетраенето и решения за управление на крайната точка, които налагат защитна конфигурация и изисквания за корекции. В допълнение, Доставчикът ще въвежда технически и оперативни контроли, които гарантират, че само познати и надеждни системи на крайния потребител могат да използват мрежите на Доставчика.

4.9 В съответствие с най-добрите практики в бранша, Доставчикът ще поддържа защити за средите на центровете за данни, където има или се обработва Материал на Kyndryl, с такива защити, включително откриване и предотвратяване на проникване и противодействие на атака срещу отказ на услуга и смекчаване.

5. Контрол на целостта и наличността на Услугата и Системите

5.1 Доставчикът ще: (a) извършва оценки на риска за сигурността и конфиденциалността най-малко веднъж годишно, (b) извършва тестване на сигурността и оценява уязвимостите, включително сканиране на сигурността на автоматичната система и приложение и ръчно етично хакерство, преди освобождаване на производството и ежегодно след това, що се отнася до Услугите и Продуктите и ежегодно по отношение на неговото боравене с Технологията на Kyndryl, (c) привлече квалифицирана независима трета страна за извършване на тестване за проникване съответстващо с най-добрите практики в бранша поне веднъж годишно, като такова тестване включва и както автоматизирано така и ръчно тестване, (d) извършване на автоматизирано ръководене и рутинна проверка за съответствие с изискванията за конфигурация на защитата за всеки компонент на Услугите и Продуктите и по отношение на неговото боравене с Технологията на Kyndryl, и (e) отстранява идентифицирани уязвимости или несъответствие с изискванията за конфигурация на защитата въз основа на асоцииран риск, експлоатационност и влияние. Доставчикът ще предприеме разумни стъпки, за да избегне прекъсване на Услугите, когато извършва своите тестове, оценки, сканирания и изпълнение на възстановителни дейности. При заявка на Kyndryl, Доставчикът ще предостави на Kyndryl писмено обобщение на най-скорошните дейности на Доставчика за тестване за проникване към момента, и този доклад, че включва най-малко името на офертите, обхванати при тестването, номера на системите или приложенията в обхвата на тестването, датите на тестване, методологията, използвана при тестването, и цялостно обобщение на констатациите.

5.2 Доставчикът ще поддържа политики и процедури, предназначени да управляват рисковете, асоциирани с приложението на промени в Услугите или Продуктите или в Боравенето с Технологията на Kyndryl. Преди прилагането на такава променя, включително на засегнати на системи, мрежи и основни компоненти, Доставчикът ще документира в регистрирана заявка на промяната: (a) описание на и причина за промяната, (b) подробности за реализацията и график, (c) изявление за риск за справяне с

въздействието върху Услугите и Продуктите, клиентите на Услугите или Материалите на Kyndryl, (d) очакван резултат, (e) план за връщане назад и (f) одобрение от оторизирани служители на Доставчика.

5.3 Доставчикът ще поддържа инвентаризация на всички IT активи, които използва при извършване на Услугите, предоставяне на Продуктите и при Боравене с Технологията на Kyndryl. Доставчикът непрекъснато ще наблюдава и управлява здравето (включително капацитет) и достъпност на такива IT активи, Услуги, Продукти и Технология на Kyndryl, включително основните компоненти на такива активи, Услуги, Продукти и Технология на Kyndryl.

5.4 Доставчикът ще изгради всички системи, които използва при разработването или експлоатация на Услуги и Продукти и при Боравенето с Технологията на Kyndryl от предварително зададени изображения за сигурност на системата или базови линии за защита, които отговарят на най-добрите практики в бранша, като например показатели на Центъра за интернет сигурност (ЦИС).

5.5 Без да се ограничават задълженията на Доставчика или правата на Kyndryl съгласно Документа по сделката или свързания базов договор между страните по отношение на непрекъснатостта на бизнеса, Доставчикът ще оцени поотделно всяка Услуга и Продукт и всяка IT система, използвана при Боравене с Технологията на Kyndryl за непрекъснатост на бизнеса и IT и за изискванията за възстановяване след бедствие в съответствие с документираните насоки за управление на риска. Доставчикът ще гарантира, че всяка такава Услуга, Продукт и IT система имат, до степента, гарантирана от такава оценка на риска, отделно определени, документирани, поддържани и ежегодно валидирани планове за бизнес и IT непрекъснатост и възстановяване след бедствие, съответстващи на най-добрите практики в бранша. Доставчикът ще гарантира, че такива планове са предназначени да предоставят специфични времеви рамки за възстановяване , които са зададени в Раздел 5.6 по-долу.

5.6 Целите за специфична точка на възстановяване ("**PRO**") и целите на времевите рамки на възстановяване („**RTO**“) по отношение на която и да е Хоствана Услуга са: 24 часа PRO и 24 часа RTO; въпреки това Доставчикът ще спазва всяко по-кратко времетраене на PRO или RTO, за което Kyndryl е поел ангажимент към Клиента, веднага след като Kyndryl уведоми писмено Доставчика за такова по-кратко времетраене на RPO или RTO (имейл представлява писмена форма). Що се отнася до всички други Услуги, предоставяни от Доставчика на Kyndryl, Доставчикът ще гарантира, че неговите планове за непрекъснатост на бизнеса и възстановяване след бедствие са предназначени да предоставят RPO и RTO, които позволяват на Доставчика да е в съответствие с всички свои задължения към Kyndryl съгласно Документа по сделката и асоциирано базово споразумение между страните, и тези Условия, включително задълженията си за своевременно предоставяне на тестване, поддръжка и профилактика.

5.7 Доставчикът ще поддържа мерки, предназначени за оценяване, тестване и прилагане на предупредителни поправки на сигурност към Услугите и Продуктите и асоциирани 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 Технологията на Kyndryl. След като се установи, че предупредителната поправка на сигурност е приложима и подходяща, Доставчикът ще въведе поправката в съответствие с документираните насоки за ниво на сериозност и оценка на риска. Въвеждането от страна на Доставчика на предупредителни поправки на сигурност ще бъде предмет на неговата политика за управление на промяната.

5.8 Ако Kyndryl има основателна причина да вярва, че хардуера или софтуера, който Доставчикът предоставя на Kyndryl, може да съдържа елементи за намеса, като шпиониращ софтуер, злонамерен софтуер или зловреден код, тогава Доставчикът своевременно ще сътрудничи на Kyndryl при разследване и отстраняване на опасенията на Kyndryl.

6. Предоставяне на Услуги

6.1 Доставчикът ще поддържа общите браншови методи за обединено разпознаване за всички потребителски или клиентски акаунти на Kyndryl, като Доставчикът ще следва най-добрите практики в бранша за удостоверяване на такива потребителски или клиентски акаунти на Kyndryl (като например централно управлявано от Kyndryl многофакторно еднократно влизане, използване на OpenID Connect (връзка чрез отворен идентификатор) или Security Assertion Markup Language (Език за маркиране на твърдение за сигурност).

7. **Подизпълнители**. Без да се ограничават задълженията на Доставчика или правата на Kyndryl съгласно Документа по сделката или свързания базов договор между страните по отношение на задържане на подизпълнителите, Доставчикът ще гарантира, че всеки подизпълнител, изпълняващ работа за Доставчика е въвел контроли на управлението, за да се спазват изискванията и задълженията, които тези Условия налагат на Доставчика.

8. **Физически носители**. Доставчикът сигурно ще изчисти физическите носители, предназначени за повторна употреба, преди такава повторна употреба, и ще разруши физическите носители, които не са предназначени за повторна употреба, в съответствие с най-добрите практики в бранша за изчистване на носители.

Член IX, Сертификати и отчети на Хостваните услуги

Този Член се прилага, ако Доставчикът предоставя Хоствана Услуга на Kyndryl.

1.1 Доставчикът ще получи следните сертификати или доклади в рамките на предвидените по-долу срокове:

Сертификати / Доклади	**Срок**
По отношение на Хостваните от Доставчика Услуги: Сертифициране за съответствие с ISO 27001, Информационни технологии, Техники за сигурност, Системи за управление на информационната сигурност, с такова сертифициране въз основа на оценката на компетентен независим одитор **Или** SOC 2 Тип 2: Отчет от компетентен независим одитор, показващ прегледа на системите на Доставчика, контролите и дейностите, в съответствие със SOC 2 Тип 2 (включително най-малко защита, поверителност и достъпност)	Доставчикът ще получи ISO 27001 сертифициране до 120 дни след датата на влизане в сила на Документа по сделката* или датата на приемане** и след това ще подновява сертифицирането въз основа на оценката на авторитетен независим одитор на всеки 12 месеца след това (с всяко подновяване спрямо тогавашната най-текуща версия на приложимия стандарт) Доставчикът ще получи SOC 2 Тип 2 отчет до 240 дни след датата на влизане в сила на Документа по сделката* или дата на приемане** и след това ще получи нов отчет от авторитетен независим одитор, показващ прегледа на системите на Доставчика, контролите и дейностите, в съответствие със SOC 2 Тип 2 (включително най-малко защита, поверителност и достъпност) на всеки 12 месеца след това * Ако към тази дата на влизане в сила, Доставчикът предоставя Хоствана Услуга ** Датата, на която Доставчикът поема задължението да предоставя Хоствана Услуга

1.2 Ако Доставчикът поиска писмено и Kyndryl одобри писмено, Доставчикът може да получи сертифициране еквивалентно по същество или отчет като споменатите по-горе, като се разбира, че времевите рамки зададени в горната таблица, ще се прилагат без промяна по отношение на сертифицирането еквивалентно по същество или отчет.

1.3 Доставчикът ще: (a) ще предостави на Kyndryl незабавно при заявка копие от всяко сертифициране и отчет, който Доставчикът е длъжен да получи и (b) незабавно ще разреши всички слабости на вътрешния контрол, забелязани по време на прегледите на SOC 2 или тези еквивалентни по същество (ако Kyndryl одобри това).

Член X, Сътрудничество, Проверка и Коригиране

Този Член се прилага, ако Доставчикът предоставя Услуги или Продукти на Kyndryl.

1. Сътрудничество с Доставчика

1.1 Ако Kyndryl има причина да се съмнява,че някои Услуги или Продукти може да са допринесли, допринасят или ще допринесат за проблеми с киберсигурността, тогава Доставчикът разумно ще сътрудничи на всяко запитване на Kyndryl по отношение на такова проблеми, включително чрез своевременен и изчерпателен отговор на искания за информация, независимо дали чрез документи, други записи, интервюта със съответния Персонал на Доставчика или други подобни.

1.2 Страните се съгласяват да: (a) предоставят при заявка на другия такава допълнителна информация, (b) изпълняват и доставят на другия такива документи и (c) извършват такива други действия и неща, каквито другата страна може разумно да поиска с цел изпълнение на намеренията на настоящите Условия и документите, посочени в настоящите Условия. Например, ако Kyndryl поиска, Доставчикът своевременно ще предостави термините за поверителност и сигурност на неговите писмени договори с Подизпълнители, обработващи Лични данни и подизпълнители, включително, когато Доставчикът има право да направи това, като предостави достъп до самите договори.

1.3 Ако Kyndryl поиска, Доставчикът ще предостави своевременно информация за държавите, в които неговите Продукти и компонентите на тези Продукти са били произведени, разработени или по друг начин доставени.

2. Проверка (както се използва по-долу, „Обект“ означава физическо местоположение, където Доставчикът хоства, обработва или по друг начин има достъп до Материали на Kyndryl)

2.1 Доставчикът ще поддържа подлежащи на проверка записи, показващи съответствие с тези Условия.

2.2 Kyndryl, сам или с външен одитор, може, при предварително писмено уведомление от 30 дни до Доставчика, да провери дали Доставчика спазва съответствие с настоящите Условия, включително чрез достъп до всеки Обект или Обекти за такива цели, въпреки че Kyndryl няма да осъществява достъп до центрове за данни където Доставчикът обработва данни на Kyndryl, освен ако има основание да вярва, че това би осигурило подходяща информация. Доставчикът ще сътрудничи на проверката на Kyndryl, включително като отговаря на заявки за информация своевременно, независимо дали това е чрез документи, други записи, интервюта със съответния Персонал на Доставчика или други подобни.Доставчикът може да предложи доказателство за придържане към одобрен кодекс на поведение или браншово сертифициране или по друг начин да предостави информация, за да покаже съответствие с тези Условия, за да се вземат под внимание от Kyndryl.

2.3 Проверка няма да се извършва повече от веднъж на всеки 12-месечен период, освен ако: (a) Kyndryl не потвърждава, че Доставчикът е отстранил опасенията възникнали в резултат на предишна проверка през 12-месечния период или (b) възникнало е нарушение на защитата и Kyndryl желае да провери съответствие със задълженията свързани с нарушаването. И в двата случая Kyndryl ще предостави същото предварително писмено уведомление от 30 дни, както е указано в Раздел 2.2 по-горе, но неотложността за справяне с нарушаване на защитата може да наложи Kyndryl да извърши проверка след по-малко от 30 дни след предварително писмено уведомление.

2.4. Регулатор или друг администратор може да упражнява същите права като Kyndryl в Раздели 2.2 и 2.3, като се разбира, че регулатор може да упражнява всички допълнителни права, които има съгласно закона.

2.5 Ако Kyndryl има разумно основание да заключи, че Доставчикът не спазва някое от настоящите Условия (независимо дали такова основание произтича от проверка съгласно настоящите Условия или по друг начин), тогава Доставчикът незабавно ще отстрани това неспазване.

3. Програма за борба с фалшифицирането

3.1 Ако Продуктите на Доставчика включват електронни компоненти (напр. твърди дискове, полупроводникови дискови устройства, памет, централни процесорни устройства, логически устройства или кабели), Доставчикът ще поддържа и следва документирана програма за предотвратяване на фалшифицирането, за да се попречи на първо място Доставчика да предоставя фалшиви компоненти на Kyndryl и второ, незабавно да се засече и отстрани всеки случай, при който Доставчикът по погрешка е предоставил фалшиви компоненти на Kyndryl. Доставчикът ще наложи същото задължение за поддръжка и следване на документирана програма за предотвратяване на фалшифицирането на всеки от своите доставчици, които предоставят електронни компоненти, които са включени в Продуктите на Kyndryl изпратени от Доставчика.

4. Коригиране

4.1 Ако Доставчикът не изпълни някое от задълженията си по настоящите Условия и това неизпълнение води до нарушаване на защитата, тогава Доставчикът ще коригира неизпълнението в своите действия и ще отстрани вредните последици от нарушаване на защитата, с такова изпълнение и отстраняване на нередностите при разумни за Kyndryl насоки и график. Ако обаче нарушаването на защитата произтича от предоставянето на Хостваната от Доставчика услуга с множество потребители и впоследствие засяга много клиенти на Доставчика, включително Kyndryl, тогава Доставчикът предвид естеството на нарушаването на защитата, ще коригира своевременно и по подходящ начин неизпълнението в дейностите си и отстрани вредните последици от нарушаването на защитата, като същевременно отделя дължимото внимание на всеки коментар на Kyndryl за такива корекции и отстраняване. Без да се засяга горепосоченото, Доставчикът трябва да извести Kyndryl без необосновано забавяне ако Доставчикът вече не може да спазва задълженията, зададени от приложимите закони за защита на данните.

4.2 Kyndryl ще има правото да участва в коригирането на всяко нарушение на защитата, спомената в Раздел 4.1, както счита за подходящо или необходимо, а Доставчикът ще носи отговорност за неговите разходи и разноски при коригиране на действията си и за разходите и разноските по възстановяването, които страните поемат по отношение на такова нарушение на защитата.

4.3 Като пример, разходите и разноските за възстановяване, свързани с нарушаване на защитата, биха могли да включват тези за откриване и разследване на нарушаването на защитата, определяне на отговорностите съгласно приложим закони и разпоредби, предоставяне на известия за нарушение, създаване и поддържане на кол-центрове, предоставяне на услуги за кредитен мониторинг и кредитно възстановяване, презареждане на данни, коригиране на дефекти на продукта (включително чрез Изходен код или друга разработка), задържане на трети страни за съдействие с горепосочените или други подобни дейности и друг разходи и разноски, които са необходими за отстраняване на вредните ефекти от нарушаване на защитата. За по-голяма яснота, разходите и разноските за възстановяване не включват загуба на печалби, бизнес загуби, намаляване на стойността, загуба на приходи, загуба на репутация или загуба на очаквани спестявания.