Članak I Poslovne kontakt informacije

Ovaj članak se primjenjuje ako Dobavljač ili Kyndryl Obrađuje BCI druge strane.

1.1 Kyndryl i Dobavljač mogu Obrađivati BCI druge strane gdje god posluju vezano za Dobavljačevu isporuku Usluga i Isporučivih materijala.

1.2 Strana:

a) neće koristiti ili otkrivati BCI druge strane za bilo kakvu drugu svrhu (radi jasnoće, nijedna strana neće Prodavati BCI druge strane niti koristiti ili otkrivati BCI druge strane za bilo kakve marketinške svrhe bez prethodnog pisanog pristanka druge strane i, tamo gdje je to potrebno, prethodnog pisanog pristanka zahvaćenih Ispitanika) i

b) odmah će na temelju pisanog zahtjeva druge strane izbrisati, izmijeniti, ispraviti, vratiti, pružiti informacije o Obradi, ograničiti Obradu ili poduzeti bilo koju drugu zatraženu razumnu radnju u pogledu BCI-ja druge strane.

1.3 Strane ne ulaze u odnos zajedničkih Voditelja obrade u pogledu međusobnog BCI-ja, i nijedna odredba Transakcijskog dokumenta neće se tumačiti ili smatrati naznakom bilo kakve namjere uspostavljanja odnosa zajedničkih Voditelja obrade.

1.4 Kyndryl-ova Izjava o privatnosti na stranici https://www.Kyndryl.com/privacy sadrži dodatne detalje o Kyndryl-ovoj Obradi BCI-ja.

1.5 Strane su implementirale i održavat će tehničke i organizacijske sigurnosne mjere kako bi zaštitili BCI druge strane od gubitka, uništavanja, izmjene, slučajnog ili neovlaštenog otkrivanja, slučajnog ili neovlaštenog pristupa i nezakonite Obrade.

1.6 Dobavljač će odmah (i ni u kojem slučaju kasnije od 48 sati) obavijestiti Kyndryl nakon što sazna za bilo kakvu povredu sigurnosti koja obuhvaća Kyndrylov BCI. Dobavljač će pružiti obavijest na e-adresi cyber.incidents@kyndryl.com. Dobavljač će Kyndryl-u pružiti razumno zatražene informacije o takvoj povredi te o statusu bilo kojih Dobavljačevih aktivnosti za ispravljanje i obnavljanje. Na primjer, razumno zatražene informacije mogu uključivati dnevnike koji pokazuju povlašteni, administrativni i drugi pristup Uređajima, sustavima ili aplikacijama, forenzičke slike Uređaja, sustava ili aplikacija te druge slične stavke u mjeri u kojoj je to relevantno za povredu ili Dobavljačevo ispravljanje i obnavljanje aktivnosti.

1.7 Tamo gdje Dobavljač samo Obrađuje Kyndryl-ov BCI i nema pristupa drugim podacima ili materijalima bilo koje vrste ili bilo kojem Kyndryl-ovom Korporativnom sustavu, ovaj članak i članak X (Suradnja, provjera i ispravljanje) su jedini članci koji se primjenjuju na takvu Obradu.

Članak II Tehničke i organizacijske mjere, Sigurnost podataka

Ovaj članak se primjenjuje ako Dobavljač Obrađuje Kyndryl-ove podatke osim Kyndryl-ovg BCI-ja. Dobavljač će udovoljiti zahtjevima ovog članka prilikom pružanja svih Usluga i Isporučivih materijala te na taj način štititi Kyndryl-ove Podatke od gubitka, uništavanja, izmjene, slučajnog ili neovlaštenog otkrivanja, slučajnog ili neovlaštenog pristupa i nezakonitih oblika obrade. Zahtjevi ovog članka obuhvaćaju sve aplikacije, platforme i infrastrukturu informacijskih tehnologija (IT) u kojoj Dobavljač radi ili upravlja pružanjem Isporučivih materijala i Usluga, uključujući sve okoline za razvoj, testiranje, hosting, podršku, operacije i okoline podatkovnog centra.

1. Upotreba podataka

1.1. Dobavljač ne smije dodavati u Kyndryl-ove Podatke ili s Kyndryl-ovim Podacima uključiti bilo koje informacije ili podatke uključujući bilo koje Osobne podatke bez Kyndryl-ovog prethodnog pisanog pristanka i Dobavljač ne smije koristiti Kyndryl-ove Podatke u bilo kojem obliku, agregirane ili drugačije, za bilo koju svrhu osim za pružanje Usluga i Isporučivih materijala Kyndryl-u (na primjer, Dobavljaču nije dozvoljeno koristiti ili ponovno koristiti Kyndryl-ove Podatke kako bi procijenio učinkovitost ili načine za poboljšanje Dobavljačevih ponuda, za istraživanje i razvoj u svrhu stvaranja novih ponuda niti za generiranje izvještaja koji se odnose na Dobavljačeve ponude). Dobavljaču je zabranjeno prodavati Kyndryl-ove Podatke osim ako to nije izričito dozvoljeno u Transakcijskom dokumentu.

1.2. Dobavljač neće umetati bilo koje tehnologije web praćenja u Isporučive materijale ili kao dio Usluga (takve tehnologije uključuju HTML5, lokalnu pohranu, oznake ili tokene treće strane i web signale) osim ako to nije izričito dozvoljeno u Transakcijskom dokumentu.

2. Zahtjevi treće strane i povjerljivost

2.1. Dobavljač neće otkrivati Kyndryl-ove Podatke trećim stranama osim na temelju pisanog ovlaštenja prethodno dobivenog od Kyndryl-a. Ako javno tijelo, uključujući bilo koje nadzorno tijelo, zahtijeva pristup Kyndryl-ovim Podacima (npr. ako Vlada SAD-a Dobavljaču uruči naredbu nacionalne sigurnosti za dobivanje Kyndryl-ovih Podataka) ili ako je otkrivanje Kyndryl-ovih Podataka na bilo koji drugi način zahtijevano zakonom, Dobavljač će pisanim putem obavijestiti Kyndryl o takvom zahtjevu ili obvezi te će Kyndryl-u dozvoliti razumnu mogućnost da ospori otkrivanje (tamo gdje zakon zabranjuje obavještavanje, Dobavljač će poduzeti korake za koje smatra da su razumno prikladni kako bi osporio zabranu i otkrivanje Kyndryl-ovih Podataka putem sudskog postupka ili drugim sredstvima).

2.2. Dobavljač će Kyndryl-u osigurati: (a) da će pristup Kyndryl-ovim Podacima imati samo oni Dobavljačevi zaposlenici kojima je taj pristup potreban za pružanje Usluga ili Isporučivih materijala i to samo u mjeri potrebnoj za pružanje Usluga i Isporučivih materijal; i (b) da je svojim zaposlenicima nametnuo obvezu povjerljivosti koja zahtijeva da ti zaposlenici koriste i otkrivaju Kyndryl-ove Podatke samo u mjeri dozvoljenoj ovim Odredbama.

3. Vraćanje ili brisanje Kyndryl-ovih Podataka

3.1. Dobavljač će, prema Kyndryl-ovoj odluci, izbrisati ili Kyndryl-u vratiti Kyndryl-ove Podatke nakon raskida ili isteka Transakcijskog dokumenta ili ranije na zahtjev Kyndryl-a. Ako Kyndryl zahtijeva brisanje, Dobavljač će tada u skladu s Najboljim postupcima u industriji učiniti da su podaci nečitljivi te da se ne mogu ponovno sastaviti ili rekonstruirati, a brisanje će potvrditi Kyndryl-u. Ako Kyndryl zahtijeva vraćanje Kyndryl-ovih Podataka, Dobavljač će to učiniti prema razumnom Kyndryl-ovom rasporedu i prema razumnim Kyndryl-ovim pisanim uputama.

Članak III, Privatnost

Ovaj članak se primjenjuje ako Dobavljač obrađuje Kyndryl-ove Osobne podatke.

1. Obrada

1.1 Kyndryl imenuje Dobavljača za Izvršitelja obrade Kyndryl-ovih Osobnih podataka isključivo u svrhu pružanja Isporučivih materijala i Usluga u skladu s Kyndryl-ovim uputama, uključujući upute sadržane u ovim Odredbama, Transakcijskom dokumentu i pridruženom osnovnom ugovoru između strana. Ako Dobavljač ne udovolji nekoj uputi, Kyndryl može otkazati zahvaćeni dio Usluga putem pisane obavijesti. Ako Dobavljač vjeruje da uputa krši neki zakon o zaštiti podataka, Dobavljač će o tome odmah i unutar propisanog i zahtijevanog vremenskog okvira obavijestiti Kyndryl.

1.2 Dobavljač će poštivati sve zakone o zaštiti podataka primjenjive na Usluge i Isporučive materijale.

1.3 U Prilogu Transakcijskog dokumenta ili u samom Transakcijskom dokumentu navedeno je sljedeće u pogledu Kyndryl-ovih Podataka:

(a) kategorije Ispitanika;
(b) vrste Kyndryl-ovih Osobnih podataka;
(c) radnje na podacima i aktivnosti Obrade;
(d) trajanje i učestalost Obrade; i
(e) popis Podizvršitelja obrade.

2. Tehničke i organizacijske mjere

2.1 Dobavljač će implementirati i održavati tehničke i organizacijske mjere navedene u članku II (Tehničke i organizacijske mjere, Sigurnost podataka) i u članku VIII (Tehničke i organizacijske mjere, Opća sigurnost), i na taj način osigurati odgovarajuću razinu sigurnosti u odnosu na rizik povezan s Uslugama i Isporučivim materijalima. Dobavljač potvrđuje i razumije ograničenja iz članka II, ovog članka III i članka VIII i pristaje na njih.

3. Prava i zahtjevi Ispitanika

3.1 Dobavljač će odmah obavijestiti Kyndryl (po rasporedu koji Kyndryl-u i drugim Voditeljima obrade omogućuje ispunjavanje njihovih zakonskih obveza) o bilo kojem zahtjevu Ispitanika koji ostvaruje bilo koja prava Ispitanika (npr. ispravak, brisanje ili blokiranje podataka) vezano uz Kyndryl-ove Osobne podatke. Dobavljač također može Ispitanika koji ima takav zahtjev odmah uputiti na Kyndryl. Dobavljač neće odgovarati na zahtjeve Ispitanika osim ako je zakonski obvezan ili ako je dobio pisanu uputu od Kyndryl-a da to učini.

3.2 Ako je Kyndryl dužan pružiti informacije o Kyndryl-ovim Osobnim podacima Drugim voditeljima obrade ili trećim stranama (npr. Ispitanicima ili Nadzornim tijelima), Dobavljač će pomoći Kyndryl-u pružanjem informacija i poduzimanjem drugih razumnih radnji koje zatraži Kyndryl, po rasporedu koji Kyndryl-u omogućuje pravovremeno odgovaranje takvim Drugim voditeljima obrade ili trećim stranama.

4. Podizvršitelji obrade

4.1 Dobavljač će unaprijed pružiti pisanu obavijest Kyndryl-u prije dodavanja novog Podizvršitelja obrade ili prije proširivanja opsega Obrade postojećeg Podizvršitelja obrade te će na takvoj pisanoj obavijesti navesti novi ili prošireni opseg Obrade. Kyndryl se može usprotiviti bilo kojem takvom novom Podizvršitelju obrade ili proširenju opsega u bilo kojem trenutku na temelju razumno opravdanih razloga, a ako to učini, strane će surađivati u dobroj vjeri kako bi našle rješenje za Kyndryl-ov prigovor. U skladu s Kyndryl-ovim pravom na prigovor u bilo kojem trenutku, Dobavljač može angažirati novog

Podizvršitelja obrade ili proširiti opseg Obrade postojećeg Podizvršitelja obrade ako Kyndryl ne uloži prigovor u roku od 30 dana od datuma Dobavljačeve pisane obavijesti.

4.2 Dobavljač će bilo kojem odobrenom Podizvršitelju obrade nametnuti obveze zaštite podataka, sigurnosti i certificiranja navedene u ovim Odredbama prije nego Podizvršitelj obrade započne obrađivati Kyndryl-ove Podatke. Dobavljač je u potpunosti Kyndryl-u odgovoran za izvršavanje obveza svakog Podizvršitelja obrade.

5. Prekogranična obrada podataka

Kako se upotrebljavaju u nastavku:

Država s primjerenom zaštitom označava državu koja pruža primjerenu razinu zaštite podataka u pogledu odgovarajućeg prijenosa sukladno primjenjivim zakonima o zaštiti podataka ili odlukama nadzornih tijela.

Uvoznik podataka označava ili Izvršitelja obrade ili Podizvršitelja obrade koji nema poslovni nastan u Državi s primjerenom zaštitom.

Standardne ugovorne klauzule Europske unije ("EU SCC-ovi") označava Standardne ugovorne klauzule Europske unije (engl. EU Standard Contractual Clauses - EU SCCs) (Odluka Komisije 2021/914) s primijenjenim izbornim klauzulama osim opcije 1 iz klauzule 9(a) i opcije 2 iz klauzule 17, koje su službeno objavljene na stranici https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en.

Standardne ugovorne klauzule Srbije ("Srpski SCC-ovi") označava Standardne ugovorne klauzule Srbije kako ih je usvojio "Srpski poverenik za informacije od javnog značaja i zaštitu podataka ličnosti" objavljene na stranici https://www.poverenik.rs/images/stories/dokumentacija-nova/podzakonski-akti/Klauzulelat.docx.

Standardne ugovorne klauzule ("**SCC-ovi"**) označava ugovorne klauzule koje su potrebne radi zakona o zaštiti podataka primjenjivih na prijenos Osobnih podataka Izvršiteljima obrade čiji se poslovni nastan ne nalazi u Državama s primjerenom zaštitom.

Dodatak o međunarodnom prijenosu podataka Ujedinjenog Kraljevstva Standardnim ugovornim klauzulama Komisije EU-a ("UK Dodatak") označava Dodatak o međunarodnom prijenosu podataka Ujedinjenog Kraljevstva Standardnim ugovornim klauzulama Komisije EU-a kako je službeno objavljeno na stranici https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-Transfer-agreement-and-guidance/.

5.1 Dobavljač neće preko granice prenositi ili otkrivati (uključujući pristup na daljinu) bilo koje Kyndryl-ove Osobne podatke bez prethodnog pisanog pristanka Kyndryl-a. Ako Kyndryl pruži takav pristanak, strane će surađivati kako bi se osigurala sukladnost s primjenjivim zakonima za zaštitu podataka. Ako ti zakoni zahtijevaju SCC-ove, Dobavljač će na Kyndryl-ov zahtjev odmah sklopiti SCC-ove.

5.2 Vezano uz EU SCC-ove:

(a) Ako Dobavljač nema poslovni nastan u Državi s primjerenom zaštitom: Dobavljač ovdje sklapa EU SCC-ove s Kyndryl-om kao Uvoznik podataka i Dobavljač će sklopiti pisane ugovore sa svakim odobrenim Podizvršiteljem obrade u skladu s klauzulom 9 EU SCC-ova te će Kyndryl-u na zahtjev pružiti pisane primjerke tih ugovora.

(i) Modul 1 EU SCC-ova se ne primjenjuje osim ako se strane nisu drugačije pisano dogovorile.

(ii) Modul 2 EU SCC-ova se primjenjuje tamo gdje je voditelj obrade Kyndryl, a Modul 3 EU SCC-ova se primjenjuje tamo gdje je Izvršitelj obrade Kyndryl. U skladu s klauzulom 13 EU SCC-ova, kad se primjenjuje Modul 2 ili Modul 3 strane se slažu (1) EU SCC-ove regulira pravo države članice EU-a u kojoj se nalazi nadležno nadzorno tijelo i (2) sporovi proizašli iz EU SCC-ova rješavat će se na sudovima države članice EU-a u kojoj se nalazi nadležno nadzorno tijelo. Ako takvo pravo iz (1) ne omogućuje prava korisnika treće strane, tada će se na EU SCC-ove primijeniti nizozemsko pravo, a svi sporovi proizašli iz EU SCC-ova temeljem (2) bit će riješeni pred sudom u Amsterdamu, Nizozemska.

(b) Ako dobavljač ima poslovni nastan u Europskom gospodarskom prostoru, a Kyndryl je voditelj obrade koji ne podliježe Općoj uredbi o zaštiti podataka 2016/679, tada se primjenjuje Modul 4 EU SCC-ova i Dobavljač ovdje kao izvoznik podataka sklapa EU SCC-ove s Kyndryl-om. Ako se primjenjuje Modul 4 EU SCC-ova, strane se slažu da se na EU SCC-ove primjenjuje nizozemsko pravo i svi sporovi proizašli iz EU SCC-ova bit će riješeni pred sudom u Amsterdamu, Nizozemska.

(c) Ako Drugi voditelji obrade poput Korisnika ili povezanih društava zatraže da postane strana u EU SCC-ovima u skladu s 'klauzulom o pristanku' u klauzuli 7, Dobavljač ovdje pristaje na svaki takav zahtjev.

(d) Tehničke i organizacijske mjere potrebne za cjelovitost Dodatka II EU SCC-ova mogu se pronaći u ovim Odredbama, samom Transakcijskom dokumentu i pridruženom osnovnom ugovoru između strana.

(e) U slučaju sukoba između EU SCC-ova i ovih Odredbi, EU SCC-ovi imaju prednost.

5.3 Vezano uz UK SCC-ove:

(a) Ako Dobavljač nema poslovni nastan u Državi s primjerenom zaštitom: (i) Dobavljač ovdje u ime Dobavljača sklapa UK SCC-ove s Kyndryl-om kao Uvoznik podataka; i (ii) Dobavljač će sklopiti pisane ugovore sa svakim odobrenim Podizvršiteljem obrade koji je Uvoznik podataka, u skladu s klauzulom 11 UK SCC-ova te će Kyndryl-u na zahtjev pružiti pisane primjerke tih ugovora.

(b) Ako Dobavljač ima poslovni nastan u Državi s primjerenom zaštitom, tada Dobavljač ovdje sklapa UK SCC-ove s Kyndryl-om u ime svakog Podizvršitelja obrade koji je Uvoznik podataka. Ako Dobavljač to ne može učiniti za bilo kojeg takvog Podizvršitelja obrade, Dobavljač će Kyndryl-u pružiti UK SCC-ove s potpisom tog Podizvršitelja obrade za Kyndryl-ov supotpis prije nego se Podizvršitelju obrade dozvoli obrađivanje bilo kojih Kyndryl-ovih Osobnih podataka.

(c) UK SCC-ovi između Kyndryl-a i Dobavljača služit će bilo kao UK SCC-ovi između Voditelja obrade i Izvršitelja obrade ili kao "leđa o leđa" (engl. back-to-back) pisani ugovor između 'uvoznika podataka' i 'podizvršitelja obrade' u skladu s klauzulom 11 iz UK SCC-ova, ovisno kako činjenice zahtijevaju. U slučaju sukoba između UK SCC-ova i ovih Odredbi, UK SCC-ovi imaju prednost.

(d) Drugi voditelji obrade poput Korisnika ili povezanih društava mogu zatražiti da postanu dodatni 'izvoznici podataka'. Dobavljač ovime pristaje u svoje ime i u ime svojih Podizvršitelja obrade na sve takve zahtjeve. Kyndryl će obavijestiti Dobavljača o svim dodatnim 'izvoznicima podataka', zatim će Dobavljač obavijestiti svoje Podizvršitelje obrade koji su Uvoznici podataka o tim dodatnim 'izvoznicima podataka'.

5.4 Vezano uz Dodatak(Dodatke) Ujedinjenog Kraljevstva:

a) Ako Dobavljač nema poslovni nastan u Državi s primjerenom zaštitom: (i) Dobavljač ovdje sklapa UK Dodatak(Dodatke) s Kyndrylom kao Uvoznik, koji se dodaje gore navedenim EU SCC-ovima (ako je primjenjivo, ovisno o okolnostima aktivnosti obrade); i (ii) Dobavljač će sklopiti pisane ugovore sa svakim odobrenim Podizvršiteljem obrade te će Kyndrylu na zahtjev dostaviti primjerke tih ugovora.

b) Ako Dobavljač ima poslovni nastan u Državi s primjerenom zaštitom, a Kyndryl je Voditelj obrade koji ne podliježe Općoj uredbi o zaštiti podataka UK-a (uključena u zakonodavstvo Ujedinjenog Kraljevstva temeljem Zakonu o povlačenju iz Europske unije iz 2018.), tada Dobavljač ovdje sklapa UK Dodatak(Dodatke) s Kyndrylom kao Izvoznik, koji se dodaje EU SCC-ovima navedenima gore u odjeljku 5.2(b).

c) Ako drugi Voditelji obrade poput Korisnika ili povezanih društava zatraže da ih se uključi u UK Dodatak(Dodatke), Dobavljač ovdje pristaje na svaki takav zahtjev.

d) Informacije priloga (kako su navedene u Tablici 3) u UK Dodatku(Dodacima) mogu se pronaći u odgovarajućim EU SCC-ovima, ovim Odredbama, samom Transakcijskom dokumentu i u pridruženom osnovnom ugovoru između strana. Ni Kyndryl ni Dobavljač ne mogu raskinuti UK Dodatak(Dodatke) kad se UK Dodatak promijeni.

e) U slučaju bilo kakvog sukoba između UK Dodatka(Dodataka) i ovih Odredbi, prednost će imati UK Dodatak(Dodaci).

5.5 Vezano uz Srpske SCC-ove:

(a) Ako Dobavljač nema poslovni nastan u Državi s primjerenom zaštitom: (i) Dobavljač ovdje u vlastito ime sklapa Srpske SCC-ove s Kyndryl-om kao Izvršitelj obrade; i (ii) Dobavljač će sklopiti pisane ugovore sa svakim odobrenim Podizvršiteljem obrade u skladu s člankom 8 Srpskih SCC-ova te će Kyndryl-u na zahtjev pružiti pisane primjerke tih ugovora.

(b) Ako Dobavljač ima poslovni nastan u Državi s primjerenom zaštitom, tada Dobavljač ovdje sklapa Srpske SCC-ove s Kyndryl-om u ime svakog Podizvršitelja obrade koji se nalazi u Državi bez primjerene zaštitom. Ako Dobavljač to ne može učiniti za bilo kojeg takvog Podizvršitelja obrade, Dobavljač će Kyndryl-u pružiti Srpske SCC-ove s potpisom tog Podizvršitelja obrade za Kyndryl-ov supotpis prije nego se Podizvršitelju obrade dozvoli obrađivanje bilo kojih Kyndryl-ovih Osobnih podataka.

(c) Srpski SCC-ovi između Kyndryl-a i Dobavljača služit će bilo kao Srpski SCC-ovi između Voditelja obrade i Izvršitelja obrade ili kao "leđa o leđa" (engl. back-to-back) pisani ugovor između ‘izvršitelja obrade’ i ‘podizvršitelja obrade’, ovisno kako činjenice zahtijevaju. U slučaju sukoba između Srpskih SCC-ova i ovih Odredbi, Srpski SCC-ovi imaju prednost.

(d) Informacije potrebne za ispunjavanje Dodataka 1 do 8 Srpskih SCC-ova koji uređuje prijenos Osobnih podataka u Državu bez primjerene zaštite mogu se pronaći u ovim Odredbama i u Prilogu Transakcijskog dokumenta ili u samom Transakcijskom dokumentu.

6. Pomoć i zapisi

6.1 Uzimajući u obzir prirodu Obrade, Dobavljač će pomoći Kyndryl-u uspostavljanjem odgovarajućih tehničkih i organizacijskih mjera za ispunjavanje obveza vezanih uz zahtjeve i prava Ispitanika. Dobavljač će također pomoći Kyndryl-u u osiguravanju usklađenosti s obvezama koje se odnose na sigurnost Obrade, obavještavanje i izvješćivanje o Povredi sigurnosti te procjeni učinaka zaštite podataka, uključujući prethodne konzultacije s odgovornim nadzornim tijelom, ako su potrebne, uzimajući u obzir informacije dostupne Dobavljaču.

6.2 Dobavljač će održavati ažurnu evidenciju naziva i kontakt detalja svakog Podizvršitelja obrade, uključujući predstavnike i službenike za zaštitu podataka svakog Podizvršitelja obrade. Na zahtjev Kyndryl-a Dobavljač će ovu evidenciju pružiti Kyndryl-u, po rasporedu koji Kyndryl-u omogućuje pravovremeno odgovaranje na bilo koji zahtjev Korisnika ili treće strane.

Članak IV Tehničke i organizacijske mjere, Sigurnost koda

Ovaj članak se primjenjuje ako Dobavljač ima pristup Kyndryl-ovom Izvornom kodu. Dobavljač će udovoljiti zahtjevima ovog članka te na taj način štititi Kyndryl-ov Izvorni kod od gubitka, uništavanja, izmjene, slučajnog ili neovlaštenog otkrivanja, slučajnog ili neovlaštenog pristupa i nezakonitih oblika rukovanja. Zahtjevi ovog članka obuhvaćaju sve aplikacije, platforme i infrastrukturu informacijskih tehnologija (IT) u kojoj Dobavljač radi ili upravlja pružanjem Isporučivih materijala i Usluga te u kojima rukuje Kyndryl-ovom Tehnologijom, uključujući sve okoline za razvoj, testiranje, hosting, podršku, operacije i centar podataka.

1. Sigurnosni zahtjevi

Kako se upotrebljavaju u nastavku:

Zabranjena država označava državu: (a) koju je Vlada SAD-a označila kao stranog protivnika temeljem Izvršnog naloga o osiguranju lanca opskrbe tehnologijama i uslugama za informacije i komunikacije (engl. Executive Order on Securing the Information and Communications Technology and Services Supply Chain) od 15. svibnja 2019., (b) stavljenu na popis u skladu s odjeljkom 1654 Zakona o nacionalnoj obrani Sjedinjenih Država (engl. U.S. National Defense Authorization Act) iz 2019. ili (c) identificiranu kao "Zabranjena država" u Transakcijskom dokumentu.

1.1. Dobavljač neće nijedan Kyndryl-ov Izvorni kod distribuirati ili davati kao zalog u korist bilo koje treće strane.

1.2. Dobavljač neće dozvoliti da se Kyndryl-ov Izvorni kod nalazi na poslužiteljima u Zabranjenoj državi. Dobavljač neće dozvoliti nikome, uključujući ni njegovom Osoblju koje se nalazi u Zabranjenoj državi ili koje posjećuje Zabranjenu državu (tijekom bilo kojeg takvog posjeta), da iz bilo kojeg razloga pristupa ili koristi bilo koji Kyndryl-ov Izvorni kod, bez obzira gdje se globalno nalazi Kyndryl-ov Izvorni kod i Dobavljač neće dozvoliti odvijanje bilo kakvog razvoja, testiranja ili drugog rada u Zabranjenoj državi, koji bi zahtijevao takav pristup ili upotrebu.

1.3. Dobavljač neće stavljati ili distribuirati Kyndryl-ov Izvorni kod u bilo kojoj pravnoj nadležnosti gdje zakon ili tumačenje zakona zahtijeva otkrivanje Izvornog koda bilo kojoj trećoj strani. Ako se promijeni zakon ili tumačenje zakona u pravnoj nadležnosti u kojoj se nalazi Kyndryl-ov Izvorni kod, zbog čega se od Dobavljača može zahtijevati da otkrije takav Izvorni kod trećoj strani, Dobavljač će odmah uništiti ili odmah ukloniti takav Kyndryl-ov Izvorni kod iz te pravne nadležnosti i neće staviti nikakav dodatni Kyndryl-ov Izvorni kod u takvu nadležnost ako takav zakon ili tumačenje zakona ostane na snazi.

1.4. Dobavljač neće, izravno ili neizravno, poduzimati radnje, uključujući sklapanje ugovora, zbog kojih bi se Dobavljač, Kyndryl ili bilo koja treća strana izvrgnula obvezi otkrivanja izvornog koda na temelju odjeljaka 1654 ili 1655 Zakona o nacionalnoj obrani Sjedinjenih Država iz 2019. Radi jasnoće, osim ako to nije izričito dozvoljeno u Transakcijskom dokumentu ili u pridruženom osnovnom ugovoru između strana, Dobavljač ne smije ni u kakvim okolnostima otkrivati Kyndryl-ov Izvorni kod bilo kojoj trećoj strani bez prethodnog pisanog pristanka Kyndryl-a.

1.5. Ako Kyndryl obavijesti Dobavljača ili ako treća strana obavijesti Kyndryl ili Dobavljača da je: (a) Dobavljač dozvolio da se Kyndryl-ov Izvorni kod donese u Zabranjenu državu ili bilo koju pravnu nadležnost koja podliježe odjeljku 1.3 iznad, (b) Dobavljač drugačije objavio, pristupio ili koristio Kyndryl-ov Izvorni kod na način koji nije dozvoljen u Transakcijskom dokumentu ili pridruženom osnovnom ili drugom ugovoru između strana ili (c) Dobavljač prekršio odjeljak 1.4 iznad, tada ne ograničavajući bilo koja druga prava Kyndryl-a za rješavanje takvog nepoštivanja sukladno zakonu ili propisima o pravičnosti ili temeljem Transakcijskog dokumenta ili pridruženog osnovnog ili drugog ugovora između strana: (i) ako takvu obavijest dobije Dobavljač, tada će Dobavljač odmah obavijestiti Kyndryl; i (ii) Dobavljač će po Kyndryl-ovim razumnim uputama istražiti i ispraviti problem prema rasporedu kojeg će Kyndryl razumno odrediti (nakon savjetovanja s Dobavljačem).

1.6. Ako Kyndryl razumno smatra da mogu biti potrebne promjene u Dobavljačevim politikama, procedurama, kontrolama ili postupcima u pogledu pristupa Izvornom kodu kako bi se riješila pitanja računalne sigurnosti, krađe intelektualnog vlasništva ili sličnih ili povezanih rizika (uključujući rizik da bez takvih promjena Kyndryl može biti ograničen kod prodavanja određenim Kupcima ili na određenim

tržištima ili na drugi način neće moći zadovoljiti sigurnost Kupca ili zahtjeve lanca opskrbe), onda Kyndryl može kontaktirati Dobavljača kako bi raspravili o radnjama koje su potrebne za rješavanje takvih rizika, uključujući promjene na takvim politikama, procedurama, kontrolama ili praksama. Na Kyndryl-ov zahtjev Dobavljač će surađivati s Kyndryl-om u procjenjivanju jesu li takve promjene potrebne kao i u implementiranju odgovarajućih, zajednički dogovorenih promjena.

Članak V Siguran razvoj

Ovaj članak se primjenjuje ako će Dobavljač Kyndryl-u pružiti svoj Izvorni kod, Izvorni kod treće strane ili Softver na lokaciji ili ako će se Dobavljačevi Isporučivi materijali ili Usluge pružati Kyndryl-ovom Korisniku u sklopu Kyndryl-ovog proizvoda ili usluge.

1. Sigurnosna spremnost

Dobavljač će surađivati u Kyndryl-ovim internim procesima koji procjenjuju sigurnosnu spremnost Kyndryl-ovih proizvoda i usluga koje ovise o bilo kojim Dobavljačevim Isporučivim materijalima, uključujući pružanje pravovremenih i potpunih odgovora o zatraženim informacijama bilo putem dokumentacije, drugih evidencija, razgovora s odgovarajućim Dobavljačevim osobljem ili slično.

2. Siguran razvoj

2.1 Ovaj odjeljak 2 se primjenjuje samo kad Dobavljač pruža Softver na lokaciji Kyndryl-u.

2.2 Dobavljač je implementirao i održavat će u skladu s Najboljim postupcima u industriji tijekom cijelog razdoblja Transakcijskog dokumenta sigurnosne politike, procedure i kontrole fokusirane na mrežu, platformu, sustav, aplikacije, uređaje, fizičku infrastrukturu, odgovore na incidente i Osoblje koje su potrebne kako bi zaštitio: (a) sustave i okoline za razvoj, izgradnju, testiranje i rad na kojima Dobavljač ili bilo koja treća strana koju je angažirao Dobavljač radi, upravlja, koristi ili se drugačije oslanja za ili u pogledu Isporučivih materijala i (b) izvorni kod svih Isporučivih materijala od gubitka, nezakonitog oblika rukovanja te neovlaštenog pristupa, otkrivanja ili izmjene.

3. ISO 20243 certifikat

3.1 Ovaj odjeljak 3 se primjenjuje samo ako će se bilo koji od Dobavljačevih Isporučivih materijala ili Usluga pružati Kyndryl-ovom Korisniku u sklopu Kyndryl-ovog proizvoda ili usluge.

3.2 Dobavljač će pribaviti certifikat usklađenosti s ISO 20243, Informacijska tehnologija, Open Trusted Technology Provider, TM Standard (O-TTPS), Otklanjanje posljedica zlonamjerno oštećenih i krivotvorenih proizvoda (bilo certificiranjem putem osobne procjene ili na bazi procjene uglednog neovisnog revizora). Druga mogućnost je, ako Dobavljač pisano zatraži, a Kyndryl pisano odobri, Dobavljač će pribaviti certifikat usklađenosti sa sadržajno ekvivalentnim industrijskim standardom koji se bavi sigurnim postupcima u razvoju i u lancu opskrbe (bilo certificiranjem putem osobne procjene ili na bazi procjene uglednog neovisnog revizora, ako Kyndryl odobri te u skladu s Kyndryl-ovim odobrenjem)

3.3 Dobavljač će pribaviti certifikat usklađenosti s ISO 20243 ili sa sadržajno ekvivalentnim industrijskim standardom (ako to pisano odobri Kyndryl) 180 dana nakon datuma stupanja na snagu Transakcijskog dokumenta i zatim obnavljati certifikate svakih 12 mjeseci nakon toga (svako obnavljanje odnosit će se na tada važeću verziju primjenjivog standarda npr. ISO 20243 ili, tamo gdje je to Kyndryl pisano odobrio, na sadržajno ekvivalentan industrijski standard koji se bavi sigurnim postupcima u razvoju i lancu opskrbe.

3.4 Dobavljač će na Kyndryl-ov zahtjev odmah pružiti primjerak certifikata koje Dobavljač treba obavezno pribaviti, a navedeni su u odjeljcima 2.1 i 2.2 iznad.

4. Sigurnosne ranjivosti

Kako se upotrebljavaju u nastavku:

Ispravak greške označava ispravke grešaka i prerade koje ispravljaju greške ili nedostatke u Isporučivim materijalima, uključujući Sigurnosne ranjivosti.

Ublažavanje označava bilo koje poznate načine umanjenja ili izbjegavanje rizika Sigurnosne ranjivosti.

Sigurnosna ranjivost označava stanje dizajna, kodiranja, razvoja, implementacije, testiranja, rada, podrške, održavanja ili upravljanja Isporučivog materijala, koje dozvoljava napad od strane bilo koga i koje može dovesti do neovlaštenog pristupa ili korištenja, uključujući: (a) pristup, kontroliranje ili prekidanje rada sustava, (b) pristup, brisanje, mijenjanje ili izdvajanje podataka ili (c) promjene identiteta, ovlaštenja ili dozvola korisnika ili administratora. Sigurnosna ranjivost može postojati bez obzira na to da li joj je dodijeljen Common Vulnerabilities and Exposures (CVE) ID ili bilo koja druga ocjena ili službena klasifikacija.

4.1 Dobavljač izjavljuje i jamči da će: (a) koristiti Najbolje postupke u industriji za identificiranje Sigurnosnih ranjivosti, uključujući neprekidno sigurnosno skeniranje statičkog i dinamičkog izvornog koda aplikacija, sigurnosno skeniranje open sourcea i skeniranje ranjivosti sustava, i (b) poštivati zahtjeve ovih Odredbi kako bi pomogao u sprječavanju, otkrivanju i ispravljanju Sigurnosnih ranjivosti u Isporučivim materijalima i u svim aplikacijama informatičke tehnologije, platformama i infrastrukturi u kojoj i kroz koju Dobavljač stvara i pruža Usluge i Isporučive materijale.

4.2 Ako Dobavljač uoči Sigurnosnu ranjivost u Isporučivom materijalu ili u bilo kojoj takvoj IT aplikaciji, platformi ili infrastrukturi, Dobavljač će Kyndryl-u pružiti Ispravak greške i Ublažavanja za sve verzije i izdanja Isporučivih materijala u skladu s Razinama ozbiljnosti i vremenskim okvirima definiranima u tablici ispod:

Razina ozbiljnosti*
Hitna sigurnosna ranjivost – je Sigurnosna ranjivost koja predstavlja ozbiljnu i potencijalno globalnu prijetnju. Kyndryl označava Hitnu sigurnosnu ranjivost vlastitom odlukom bez obzira na CVSS osnovnu ocjenu.
Kritična – je Sigurnosna ranjivost čija je CVSS osnovna ocjena od 9 do 10.0
Visoka – je Sigurnosna ranjivost čija je CVSS osnovna ocjena od 7.0 do 8.9
Srednja – je Sigurnosna ranjivost čija je CVSS osnovna ocjena od 4.0 do 6.9
Niska – je Sigurnosna ranjivost čija je CVSS osnovna ocjena od 0.0 do 3.9

Vremenski okviri				
Hitna	***Kritična***	***Visoka***	***Srednja***	***Niska***
4 dana ili manje, kako odredi Kyndryl-ov glavni ured za informacijsku sigurnost	30 dana	30 dana	90 dana	Sukladno Najboljim postupcima u industriji

* U bilo kojem slučaju gdje Sigurnosna ranjivost nema odmah dodijeljenu CVSS osnovnu ocjenu, Dobavljač će primijeniti razinu ozbiljnosti koja je odgovarajuća za prirodu i okolnosti takve ranjivosti.

4.3 Za Sigurnosnu ranjivost koja je javno objavljena i za koju Dobavljač još nije Kyndryl-u pružio Ispravak greške ili Ublažavanje, Dobavljač će implementirati bilo koje tehnički izvedive dodatne sigurnosne kontrole koje mogu ublažiti rizike ranjivosti.

4.4 Ako je Kyndryl nezadovoljan s Dobavljačevim odgovorom na bilo koju Sigurnosnu ranjivost u Isporučivom materijalu ili u bilo kojoj aplikaciji, platformi ili infrastrukturi na koju se upućuje iznad, tada ne dovodeći u pitanje bilo koja druga Kyndryl-ova prava, Dobavljač će odmah dogovoriti da Kyndryl raspravi svoje zabrinutosti izravno s Dobavljačevim zamjenikom predsjednika Uprave ili odgovarajućim izvršnim direktorom koji je odgovoran za isporuku Ispravka greške.

4.5 Primjeri Sigurnosnih ranjivosti uključuju kod treće strane ili open source code za koji se više ne pružaju usluge (end-of-service - EOS) pa se za te vrste koda više ne dobivaju sigurnosni popravci.

Članak VI Pristup korporativnim sustavima

Ovaj članak se primjenjuje ako će Dobavljačevi zaposlenici imati pristup bilo kojem Korporativnom sustavu.

1. Opće odredbe

1.1 Kyndryl će odrediti da li će ovlastiti Dobavljačeve zaposlenike za pristupanje Korporativnim sustavima. Ako Kyndryl izda takvo ovlaštenje, tada će Dobavljač poštivati i zahtijevat će da njegovi zaposlenici s pravom pristupa poštuju zahtjeve ovog članka.

1.2 Kyndryl će odrediti sredstva putem kojih Dobavljačevi zaposlenici mogu pristupati Korporativnim sustavima, uključujući da li će takvi zaposlenici pristupati Korporativnim sustavima putem Kyndryl-ovih uređaja ili putem uređaja koje je osigurao Dobavljač.

1.3 Dobavljačevi zaposlenici mogu pristupati Korporativnim sustavima i mogu koristiti Uređaje koje je Kyndryl autorizirao za takav pristup, ali samo za pružanje Usluga. Dobavljačevi zaposlenici ne smiju koristiti Uređaje koje je autorizirao Kyndryl za pružanje usluga bilo kojoj drugoj osobi ili pravnom subjektu ili za pristup bilo kojim IT sustavima, mrežama, aplikacijama, web stranicama, alatima e-pošte, alatima suradnje ili sličnome u vlasništvu Dobavljača ili treće strane.

1.4 Radi jasnoće, Dobavljačevi zaposlenici ne smiju koristiti Uređaje koje je Kyndryl autorizirao za pristup Korporativnim sustavima iz bilo kojih osobnih razloga (npr. Dobavljačevi zaposlenici ne smiju pohranjivati osobne datoteke poput glazbe, videa, slika ili sličnih materijala na takve Uređaje i ne mogu putem takvih Uređaja koristiti Internet iz osobnih razloga).

1.5 Dobavljačevi zaposlenici neće kopirati Kyndryl-ove Materijale koji su dohvatljivi kroz Korporativni sustav bez Kyndryl-ovog prethodnog pisanog odobrenja (i nikad neće kopirati bilo koje Kyndryl-ove Materijale na prenosivi uređaj za pohranu kao što je USB, vanjski tvrdi disk ili slično).

1.6 Na zahtjev, Dobavljač će za svakog zaposlenika poimence navesti Korporativne sustave kojima je ovlašten pristupiti i kojima je pristupio tijekom bilo kojeg vremenskog perioda kojeg odredi Kyndryl.

1.7 Dobavljač će u roku dvadeset četiri (24) sata obavijestiti Kyndryl ako neki Dobavljačev zaposlenik s pristupom bilo kojem Korporativnom sustavu: (a) više nije zaposlenik Dobavljača ili (b) više ne radi na aktivnostima koje zahtijevaju takav pristup. Dobavljač će surađivati s Kyndryl-om kako bi se odmah ukinuo pristup takvim bivšim ili sadašnjim zaposlenicima.

1.8 Dobavljač će odmah obavijestiti o svim stvarnim ili sumnjivim sigurnosnim incidentima (poput gubitka Kyndryl-ovog ili Dobavljačevog Uređaja ili neovlaštenog pristupa Uređaju ili podacima, materijalima ili drugim informacijama bilo koje vrste) Kyndryl i s Kyndryl-om će surađivati u istrazi takvih incidenata.

1.9 Dobavljač ne smije dozvoliti nijednom agentu, neovisnom pružatelju usluga ili zaposleniku podugovarača da pristupi bilo kojem Korporativnom sustavu bez prethodnog Kyndryl-ovog pisanog pristanka; ako Kyndryl pruži takav pristanak, tada će Dobavljač takve osobe i njihove poslodavce ugovorno obvezati na poštivanje zahtjeva iz ovog članka kao da su te osobe Dobavljačevi zaposlenici i Dobavljač će biti Kyndryl-u odgovoran za sve radnje ili propuste takvih osobe ili njihovog poslodavca u pogledu pristupa Korporativnom sustavu.

2. Softver uređaja

2.1 Dobavljač će uputiti svoje zaposlenik da na vrijeme instaliraju sav softver Uređaja koji Kyndryl zahtijeva za omogućavanje sigurnog pristupa Korporativnim sustavima. Ni Dobavljač ni njegovi zaposlenici neće ometati radnje tog softvera niti sigurnosne funkcije koje softver omogućuje.

2.2 Dobavljač i njegovi zaposlenici pridržavat će se pravila konfiguracije Uređaja koja postavi Kyndryl i inače će surađivati s Kyndryl-om kako bi pomogli osigurati da softver funkcionira onako kako je to namijenio Kyndryl. Na primjer, Dobavljač neće nadjačati funkciju blokiranja softverskih web stranica ili funkcije automatskog popravljanja.

2.3 Dobavljačevi zaposlenici ne smiju s bilo kojom drugom osobom dijeliti Uređaje koje koriste za pristup Korporativnim sustavima niti svoja korisnička imena, lozinke i slično.

2.4 Ako Kyndryl ovlasti Dobavljačeve zaposlenike da pristupaju Korporativnim sustavima koristeći Dobavljačeve Uređaje, tada će Dobavljač instalirati i izvoditi operativni sustav na takvim Uređajima koje je odobrio Kyndryl te će takve uređaje nadograditi na novu verziju tog operativnog sustava ili na novi operativni sustav unutar razumnog vremena nakon što dobije takvu uputu od Kyndryl-a.

3. Nadzor i suradnja

3.1 Kyndryl ima nekvalificirana prava praćenja i otklanjanja potencijalnih upada i drugih računalnih prijetnji na bilo koje načine, iz bilo kojih lokacija i korištenjem kojih god sredstava za koje Kyndryl smatra da su potrebna ili prikladna, bez upućivanja prethodne obavijesti Dobavljaču, Dobavljačevom zaposleniku ili drugima. Kao primjer takvih prava, Kyndryl može u bilo kojem trenutku, (a) provesti sigurnosno testiranje na bilo kojem Uređaju, (b) pratiti, obnoviti putem tehničkih ili drugih sredstava i pregledati komunikacije (uključujući e-poruke iz bilo kojih računa e-pošte), zapise, datoteke i druge stavke pohranjene u bilo kojem Uređaju ili prenesene kroz bilo koji Korporativni sustav i (c) dobiti potpunu forenzičku sliku bilo kojeg Uređaja. Ako Kyndryl treba suradnju Dobavljača za ostvarivanje svojih prava, Dobavljač će u potpunosti i pravovremeno udovoljiti Kyndryl-ovim zahtjevima za takvu suradnju (uključujući, na primjer, zahtjeve za sigurno konfiguriranje bilo kojeg Uređaja, instaliranje praćenja ili drugog softvera na bilo kojem Uređaju, dijeljenje detalja o povezivanju na razini sustava, angažiranje na mjerenju odgovora na incident na bilo kojem Uređaju i pružanje fizičkog pristupa bilo kojem Uređaju kako bi Kyndryl dobio potpunu forenzičku sliku ili na drugačijim, ali sličnim i povezanim zahtjevima).

3.2 Kyndryl u bilo kojem trenutku može ukinuti pristup Korporativnim sustavima bilo kojem Dobavljačevom zaposleniku ili svim Dobavljačevim zaposlenicima, bez prethodne obavijesti Dobavljaču ili bilo kojem Dobavljačevom zaposleniku ili trećim osobama, ako Kyndryl smatra da je to potrebno kako bi se zaštitio Kyndryl.

3.3 Kyndryl-ova prava ne blokiraju, ne umanjuju niti ograničavaju na bilo koji način odredbe Transakcijskog dokumenta, pridruženog osnovnog ugovora između strana ili bilo kojeg drugog ugovora između strana, uključujući bilo koju odredbu koja može zahtijevati da se podaci, materijali ili druge informacije bilo koje vrste nalaze na izabranoj lokaciji ili lokacijama ili koja može zahtijevati da samo osobe iz izabrane lokacije ili lokacija pristupaju takvim podacima, materijalima ili drugim informacijama.

4. Kyndryl-ovi Uređaji

4.1 Kyndryl će zadržati u vlasništvu sve Kyndryl-ove Uređaje, a Dobavljač će snositi rizik gubitka Uređaja, uključujući razloge poput krađe, vandalizma ili nemara. Dobavljač neće izmijeniti niti će dozvoliti izmjene na Kyndryl-ovim Uređajima bez prethodnog Kyndryl-ovog pisanog odobrenja, gdje se izmjenom smatra bilo koja promjena na Uređaju, uključujući bilo koju promjenu na softveru Uređaja, aplikacijama, sigurnosnom dizajnu, sigurnosnoj konfiguraciji ili fizičkom, mehaničkom ili električnom dizajnu.

4.2 Dobavljač će vratiti sve Kyndryl-ove Uređaje u roku 5 radnih dana nakon što više nisu potrebni za pružanje Usluga i ako Kyndryl zahtijeva Dobavljač će istodobno uništiti sve podatke, materijale i druge informacije bilo koje vrste koji se nalaze na tim Uređajima bez zadržavanja kopije, pri tom će slijediti Najbolje postupke u industriji za trajno brisanje svih takvih podataka, materijala i drugih informacija. Dobavljač će zapakirati i vratiti Kyndryl-ove Uređaje o svom trošku i u istom stanju u kojem su dostavljeni Dobavljaču osim redovnog habanja, na lokaciju koju će odrediti Kyndryl. Dobavljačevo ne poštivanje bilo koje obveze iz ovog odjeljka 4.2 predstavlja kršenje bitnih obveza iz Transakcijskog dokumenta i pridruženog osnovnog ugovora te bilo kojeg povezanog ugovora između strana, uz razumijevanje da je ugovor "povezan" ako pristup bilo kojem Korporativnom sustavu omogućava Dobavljačeve zadatke ili druge aktivnosti u okviru tog ugovora.

4.3 Kyndryl će pružiti podršku za Kyndryl-ove Uređaje (uključujući pregled Uređaja te preventivno i korektivno održavanje). Dobavljač će na vrijeme obavijestiti Kyndryl o potrebi korektivnog servisa.

4.4 Kyndryl Dobavljaču dodjeljuje privremeno pravo korištenja, pohrane i kreiranja dovoljnog broja kopija softverskih programa u vlasništvu Kyndryl-a ili za koje Kyndryl ima pravo na licencu, koji će podržati Dobavljačevu ovlaštenu upotrebu Kyndryl-ovih Uređaja. Dobavljač ne smije prenijeti programe na bilo koga, izrađivati kopije informacija softverskih licenci ili obrnuto sastavljati, obrnuto kompilirati, provoditi obrnuti inženjering ili na drugi način prevoditi bilo koji program, osim ako to izričito nije dozvoljeno mjerodavnim pravom bez mogućnosti ugovornog odricanja.

5. Ažuriranja

5.1 Bez obzira na bilo što suprotno u Transakcijskom dokumentu ili pridruženom osnovnom ugovoru između strana, putem pisane obavijesti Dobavljaču, ali bez potrebe dobivanja Dobavljačevog pristanka, Kyndryl može ažurirati, dopuniti ili na drugi način izmijeniti ovaj članak kako bi se riješio bilo koji zahtjev na temelju primjenjivog prava ili obveze Korisnika, odrazio razvoj Najboljih sigurnosnih postupaka ili na drugi način, ako Kyndryl smatra da je potrebno, zaštitili Korporativni sustavi ili Kyndryl.

Članak VII, Povećanje osoblja

Ovaj članak se primjenjuje tamo gdje će Dobavljačevo osoblje cijelo svoje radno vrijeme pružati Usluge Kyndryl-u, pružati sve Usluge u Kyndryl-ovim prostorima, prostorima Korisnika ili iz svojih domova i pružati će Usluge koristeći samo Kyndryl-ove Uređaje za pristup Korporativnim sustavima.

1. Pristup Korporativnim sustavima; Kyndryl-ove okoline

1.1 Dobavljač može pružati Usluge samo ako Korporativnim sustavima pristupa putem Uređaja koji pruži Kyndryl.

1.2 Dobavljač će poštovati odredbe navedene u članku VI (Pristup Korporativnim sustavima) prilikom svakog pristupa Korporativnim sustavima.

1.3 Uređaji koje je pružio Kyndryl su jedini Uređaji koje Dobavljač i njegovi zaposlenici mogu koristiti za pružanje Usluga, a mogu ih koristiti samo Dobavljač i njegovi zaposlenici kad pružaju Usluge. Radi jasnoće, ni u kojem slučaju Dobavljač ili njegovi zaposlenici ne smiju koristiti bilo koje druge uređaje za pružanje Usluga ili koristiti Kyndryl-ove Uređaje za bilo kojeg drugog Dobavljačevog korisnika ili za bilo koju svrhu osim pružanja Usluga Kyndryl-u.

1.4 Dobavljačevi zaposlenici koji koriste Kyndryl-ove Uređaje mogu međusobno dijeliti Kyndryl-ove Materijale i takve materijale pohraniti na Kyndryl-ove Uređaje, ali samo u ograničenoj mjeri u kojoj je takvo dijeljenje i pohranjivanje potrebno za uspješno pružanje Usluga.

1.5 Ni u kojem slučaju Dobavljač ili njegovi zaposlenici ne smiju ukloniti bilo koje Kyndryl-ove Materijale iz Kyndryl-ovih repozitorija, okolina, alata ili infrastrukture u kojoj ih drži Kyndryl, osim kad je riječ o pohrani unutar Kyndryl-ovih Uređaja.

1.6 Radi jasnoće, Dobavljač i njegovi zaposlenici nisu ovlašteni za prijenos bilo kojih Kyndryl-ovih Materijala u bilo koje Dobavljačeve repozitorije, okoline, alate ili infrastrukturu ili na bilo koje druge Dobavljačeve sustave, platforme, mreže ili slično bez Kyndryl-ovog prethodnog pisanog pristanka.

1.7 Članak VIII (Tehničke i organizacijske mjere, Opća sigurnost) se ne primjenjuje na Dobavljačeve usluge kod kojih će Dobavljačevo osoblje cijelo svoje radno vrijeme pružati Usluge Kyndryl-u, izvoditi sve Usluge u Kyndryl-ovim prostorima, prostorima Korisnika ili iz svojih domova i kad će pružati Usluge koristeći samo Kyndryl-ove Uređaje za pristup Korporativnim sustavima. Inače se članak VIII primjenjuje na Dobavljačeve Usluge.

Članak VIII Tehničke i organizacijske mjere, Opća sigurnost

Ovaj članak se primjenjuje ako Dobavljač pruža bilo koje Usluge ili Isporučive materijale Kyndryl-u, osim kad Dobavljač ima pristup samo Kyndryl BCI-ju tijekom pružanja tih Usluga i Isporučivih materijala (npr. Dobavljač neće obrađivati nikakve druge Kyndryl-ove Podatke ili neće imati pristup bilo kojim drugim Kyndryl-ovim Materijalima ili Korporativnim sustavima), Dobavljačeve Usluge i Isporučivi materijali služe za pružanje Softver na lokaciji Kyndryl-u ili Dobavljač pruža sve svoje Usluge i Isporučive materijale po modelu proširenja osoblja sukladno članku VII, uključujući od toga odjeljak 1.7.

Dobavljač će udovoljiti zahtjevima ovog članka te na taj način štititi: (a) Kyndryl-ove Materijale od gubitka, uništavanja, izmjene, slučajnog ili neovlaštenog otkrivanja i slučajnog ili neovlaštenog pristupa, (b) Kyndryl-ove Podatke od nezakonitih oblika Obrade i (c) Kyndryl-ovu Tehnologiju od nezakonitih oblika rukovanja. Zahtjevi ovog članka obuhvaćaju sve aplikacije, platforme i infrastrukturu informacijskih tehnologija (IT) u kojoj Dobavljač radi ili upravlja pružanjem Isporučivih materijala i Usluga te u kojima rukuje Kyndryl-ovom Tehnologijom, uključujući sve okoline za razvoj, testiranje, hosting, podršku, operacije i centar podataka.

1. Politike sigurnosti

1.1. Dobavljač će održavati i slijediti IT sigurnosne politike i procedure koje su sastavni dio Dobavljačevog poslovanja, obavezne za cjelokupno Dobavljačevo osoblje i usklađene s Najboljim postupcima u industriji.

1.2. Dobavljač će preispitati svoje IT sigurnosne politike i procedure najmanje jednom godišnje te ih prema potrebi ispraviti i dopuniti kako bi zaštitio Kyndryl-ove Materijale.

1.3. Dobavljač će održavati i slijediti standardne obvezne zahtjeve provjere prilikom zapošljavanja novih zaposlenika i proširiti će takve zahtjeve na Dobavljačevo osoblje i povezana društva u potpunom Dobavljačevom vlasništvu. Ti zahtjevi će uključivati provjere kažnjavanosti u prošlosti u mjeri dozvoljenoj lokalnim pravom, dokaz provjere identiteta te bilo koje dodatne provjere za koje Dobavljač smatra da su potrebne. Dobavljač će periodički ponavljati provjeru tih zahtjeva ako smatra da je to potrebno.

1.4. Dobavljač će svojem osoblju svake godine pružiti edukaciju o sigurnosti i privatnosti te će svake godine od svojeg osoblja tražiti potvrdu da će se pridržavati Dobavljačevog etičnog poslovnog ponašanja i politika čuvanja tajnosti i sigurnosti navedenih u Dobavljačevom kodeksu ponašanja ili sličnim dokumentima. Dodatnu obuku iz politika i postupanja Dobavljač će pružiti osoblju s administrativnim pristupom bilo kojoj komponenti Usluga, Isporučivih materijala ili Kyndryl-ovih Materijala, gdje će takva obuka biti specifična za njihovu ulogu i podršku Usluga, Isporučivih materijala i Kyndryl-ovih Materijala i kakva je potrebna za održavanje zahtijevane sukladnosti i certifikata.

1.5. Dobavljač će dizajnirati mjere sigurnosti i privatnosti kako bi zaštitio i održavao dostupnost Kyndryl-ovih Materijala te će kroz njihovu implementaciju, održavanje i sukladnost s politikama i procedurama koje po svojem obliku zahtijevaju sigurnost i privatnost osigurati inženjering i operacije za sve Usluge i Isporučive materijale i za svo Rukovanje Kyndryl-ovom Tehnologijom.

2. Sigurnosni incidenti

2.1. Dobavljač će održavati i slijediti dokumentirane politike odgovora na incidente sukladne Najboljim postupcima u industriji za postupanje kod sigurnosnih incidenata vezanih uz računala.

2.2. Dobavljač će provjeravati neovlašteni pristup ili neovlaštenu upotrebu Kyndryl-ovih Materijala te će definirati i izvršiti odgovarajući plan odgovora.

2.3. Dobavljač će odmah (i ni u kojem slučaju kasnije od 48 sati) obavijestiti Kyndryl nakon što sazna za bilo kakvu povredu sigurnosti. Dobavljač će pružiti obavijest na e-adresi cyber.incidents@kynrdryl.com. Dobavljač će Kyndryl-u pružiti razumno zatražene informacije o takvoj povredi te o statusu bilo kojih Dobavljačevih aktivnosti za ispravljanje i obnavljanje. Na primjer, razumno zatražene informacije mogu uključivati dnevnike koji pokazuju povlašteni, administrativni i drugi pristup Uređajima, sustavima ili aplikacijama, forenzičke slike Uređaja, sustava ili aplikacija te druge slične stavke u mjeri u kojoj je to relevantno za povredu ili Dobavljačevo ispravljanje i obnavljanje aktivnosti.

2.4. Dobavljač će Kyndryl-u pružiti razumnu pomoć u ispunjavanju bilo kojih zakonskih obveza (uključujući obveze obavještavanja Nadzornih tijela ili Ispitanika) Kyndryl-a, Kyndryl-ovih povezanih društava i Korisnika (i njihovih korisnika i povezanih društava) vezano uz Povredu sigurnosti.

2.5. Dobavljač neće informirati ili obavijestiti treću stranu da je Povreda sigurnosti izravno ili neizravno povezana s Kyndryl-om ili Kyndryl-ovim Materijalima osim ako je to pisano odobrio Kyndryl ili ako je to propisano zakonom. Dobavljač će pisano obavijestiti Kyndryl prije distribuiranja bilo kakve zakonski propisane obavijesti trećoj strani gdje bi obavijest izravno ili neizravno otkrila Kyndryl-ov identitet.

2.6. U slučaju Povrede sigurnosti koja nastane zbog Dobavljačevog kršenja bilo koje obveze temeljem ovih Odredbi:

(a) Dobavljač će biti odgovoran za sve troškove koji nastanu kao i za stvarne troškove kojima se izloži Kyndryl tijekom obavještavanja odgovarajućih Nadzornih tijela, drugih javnih tijela te samoregulirajućih agencija relevantnih djelatnosti, medija (ako to zahtijeva primjenjivo pravo), Ispitanika, Korisnika i drugih o Povredi sigurnosti,

(b) na zahtjev Kyndryl-a, Dobavljač će uspostaviti i održavati o svom vlastitom trošku pozivni centar koji će odgovarati na pitanja Ispitanika o Povredi sigurnosti i posljedicama toga, u trajanju od 1 godine od datuma kad su Ispitanici obaviješteni o Povredi sigurnosti ili u trajanju koje određuju odgovarajući mjerodavni propisi o zaštiti podataka, ovisno što od toga pruža veću zaštitu. Kyndryl i Dobavljač će surađivati na izradi skripta i drugih materijala koje će koristiti osoblje pozivnog centra prilikom odgovaranja na pitanja. Alternativno, nakon pisane obavijesti Dobavljaču, Kyndryl može umjesto Dobavljača uspostaviti i održavati svoj vlastiti pozivni centar, a Dobavljač će Kyndryl-u nadoknaditi stvarne troškove kojima se izložio Kyndryl prilikom uspostavljanja i održavanja takvog pozivnog centra, i

(c) Dobavljač će Kyndryl-u nadoknaditi stvarne troškove kojima se izloži Kyndryl tijekom pružanja usluga nadziranja i/ili vraćanja odobrenja u trajanju od 1 godine od datuma kad su pojedinci zahvaćeni povredom podataka obaviješteni o Povredi sigurnosti, a odlučili su se registrirati za takve usluge ili u trajanju koje određuju odgovarajući mjerodavni propisi o zaštiti podataka, ovisno što od toga pruža veću zaštitu.

3. Fizička sigurnost i kontrola ulaska (kako se koristi u nastavku, "Objekt" označava fizičku lokaciju na kojoj Dobavljač pruža hosting, obrađuje ili na drugi način pristupa Kyndryl-ovim Materijalima).

3.1. Dobavljač će održavati odgovarajuće fizičke kontrole pristupa poput prepreka, pristupnih točaka kontroliranih karticama, nadzornih kamera i recepcija s ljudskim osobljem kako bi zaštitio svoje Objekte od neovlaštenog ulaska.

3.2. Dobavljač će zahtijevati ovlašteno odobrenje za pristup Objektima i kontroliranim područjima unutar Objekata, uključujući bilo kakav privremeni pristup, a pristup će biti ograničen prema poslovnoj funkciji i potrebi posla. Ako Dobavljač dozvoli privremeni pristup, njegov ovlašteni zaposlenik će pratiti svakog posjetitelja tijekom njegovog zadržavanja u Objektu i u svim kontroliranim područjima.

3.3. Dobavljač će implementirati kontrole fizičkog pristupa, uključujući višeparametarske kontrole pristupa sukladne Najboljim postupcima u industriji, kako bi prikladno ograničio pristup kontroliranim područjima unutar Objekata, zabilježio sve pokušaje ulaska i takve dnevnika održavao najmanje godinu dana.

3.4. Dobavljač će ukinuti pristup Objektima i kontroliranim područjima unutar Objekata nakon (a) prestanka radnog odnosa ovlaštenog Dobavljačevog zaposlenika ili (b) kad ovlaštenom Dobavljačevom zaposleniku pristup više nije potreban radi valjanih poslovnih potreba. Dobavljač će slijediti formalne dokumentirane postupke prilikom prestanka radnog odnosa koji uključuju hitno uklanjanje iz popisa kontrole pristupa i predaju iskaznica za fizički pristup.

3.5. Dobavljač će poduzeti mjere opreza kako bi zaštitio svu fizičku infrastrukturu koja se koristi za pružanje Usluga i Isporučivih materijala od okolišnih prijetnji, koje se događaju prirodno i utjecajem čovjeka, poput prekomjerne temperature okoline, požara, poplave, vlage, krađe i vandalizma.

4. Kontrola pristupa, intervencije, prijenosa i odvajanja

4.1. Dobavljač će održavati dokumentaciju sigurnosne arhitekture mreža kojima upravlja tijekom pružanja Usluga, opskrbe Isporučivim materijalima i Rukovanja Kyndryl-ovom Tehnologijom. Dobavljač će zasebno pregledati takve mrežne arhitekture i upotrebljavati mjere sprječavanja neovlaštenih mrežnih povezivanja na sustave, aplikacije i mrežne uređaje kako bi osigurao sukladnost sa sveobuhvatnim standardnima sigurne segmentacije, izolacije i obrane. Dobavljač ne može koristiti bežičnu tehnologiju

u svom hostingu i operacijama bilo kojih Hostiranih usluga; inače, Dobavljač može koristiti bežičnu mrežnu tehnologiju prilikom pružanja Usluga i Isporučivih materijala i tijekom Rukovanja Kyndryl-ovom Tehnologijom, ali tada će Dobavljač šifrirati i zahtijevati sigurnu provjeru identiteta za bilo koju takvu bežičnu mrežu.

4.2. Dobavljač će održavati mjere namijenjene za logičko odvajanje i sprječavanja otkrivanja ili pristupa neovlaštenih osoba Kyndryl-ovim Materijalima. Nadalje, Dobavljač će održavati odgovarajuću izolaciju svojih proizvodnih, neproizvodnih i drugih okolina i, ako su Kyndryl-ovi Materijali već prisutni ili ako su preneseni u neproizvodnu okolinu (na primjer kako bi se ponovno proizvela greška), tada će Dobavljač osigurati da su sve sigurnosne zaštite i zaštite privatnosti u neproizvodnoj okolini jednake onima u proizvodnoj okolini.

4.3. Dobavljač će šifrirati Kyndryl-ove Materijale u tranzitu i u mirovanju (osim ako Dobavljač na Kyndryl-ovo razumno zadovoljstvo pokaže da je šifriranje Kyndryl-ovih Materijala u mirovanju tehnički neizvedivo). Dobavljač će također šifrirati sve fizičke medije, poput medija koji sadrže sigurnosne kopije, ako takvi postoje. Dobavljač će održavati dokumentaciju o postupcima za generiranje, izdavanje, distribuiranje, pohranu, rotiranje, povlačenje, vraćanje, sigurnosno kopiranje, uništavanje, pristup i upotrebu sigurnosnih ključeva vezanih uz šifriranje podataka. Dobavljač će osigurati da korištene specifične kriptografske metode za šifriranje slijede Najbolje postupke u industriji (poput NIST SP 800-131a).

4.4. Ako je Dobavljaču potreban pristup Kyndryl-ovim Materijalima, Dobavljač će smanjiti i ograničiti takav pristup na najmanju razinu koja je potrebna za pružanje i podršku Uslugama i Isporučivim materijalima. Dobavljač će zahtijevati da takav pristup, uključujući administrativni pristup bilo kojim osnovnim komponentama (npr. povlašteni pristup), bude pojedinačan na temelju radne funkcije te da podliježe odobrenju i redovnoj provjeri od strane ovlaštenih Dobavljačevih zaposlenika na temelju načela odvajanja dužnosti. Dobavljač će održavati mjere za identificiranje i uklanjanje suvišnih i nekorištenih računa. Dobavljač će također ukinuti račune s povlaštenim pristupom unutar dvadeset četiri (24) sata od prestanka radnog odnosa vlasnika računa ili na zahtjev Kyndryl-a ili bilo kojeg ovlaštenog Dobavljačevog zaposlenika, na primjer, na zahtjev rukovoditelja vlasnika računa.

4.5. U skladu s Najboljim postupcima u industriji, Dobavljač će održavati tehničke mjere provedbe vremenskog ograničenja neaktivnih sesija, zaključavanja računa nakon višestrukih uzastopnih neuspjelih pokušaja prijave, provjere identiteta putem jake lozinke ili pristupnog izraza i mjere koje zahtijevaju siguran prijenos i pohranu takvih lozinki i pristupnih izraza. Osim toga, Dobavljač će koristiti višeparametarsku provjeru identiteta za sve povlaštene pristupe bilo kojim Kyndryl-ovim Materijalima koji ne idu preko konzole.

4.6. Dobavljač će nadgledati upotrebu povlaštenog pristupa i održavati informacije o sigurnosti i mjere upravljanja događajima namijenjene za: (a) prepoznavanje neovlaštenog pristupa i aktivnosti, (b) olakšavanje pravovremenog i prikladnog odgovora na takav pristup i aktivnost, i (c) omogućavanje revizije usklađenosti s dokumentiranom politikom Dobavljača koju provodi Dobavljač, Kyndryl (sukladno njegovim pravima provjere u ovim Odredbama i pravima na reviziju iz Transakcijskog dokumenta ili pridruženog osnovnog ili drugog povezanog ugovora između strana) i drugi.

4.7. Dobavljač će zadržavati dnevnike u koje će u skladu s Najboljim postupcima u industriji zapisivati sve administratorske, korisničke ili druge pristupe ili aktivnosti prema ili vezane uz sustave korištene za pružanje Usluga ili Isporučivih Materijala i Rukovanje Kyndryl-ovom Tehnologijom (i te će dnevnike, na zahtjev, pružiti Kyndryl-u). Dobavljač će održavati mjere namijenjene za zaštitu od neovlaštenog pristupa, izmjene i slučajnog ili namjernog uništenja takvih dnevnika.

4.8. Dobavljač će održavati računalne zaštite za sustave u svom vlasništvu ili kojima upravlja, uključujući sustave krajnjih korisnika, koje koristi za pružanje Usluga ili Isporučivih materijala ili za Rukovanje Kyndryl-ovom Tehnologijom, sa zaštitama koje uključuju, ali nisu ograničene na: vatrozide krajnjih točaka, šifriranje cijelog diska, detektiranje krajnjih točaka na bazi potpisa i bez potpisa i tehnologije odgovora za postupanje sa zlonamjernim softverom i naprednim stalnim prijetnjama, vremensko zaključavanje ekrana i rješenja upravljanja krajnjim točkama koja provode zahtjeve konfiguracije i nadogradnje sigurnosti. Osim toga, Dobavljač će implementirati tehničke i operativne kontrole koje će osigurati da dozvolu korištenja Dobavljačevih mreža imaju poznati i pouzdani sustavi krajnjih korisnika.

4.9. U skladu s Najboljim postupcima u industriji, Dobavljač će štititi okoline centra podataka u kojoj se nalaze ili obrađuju Kyndryl-ovi Materijali, sa zaštitama koje uključuju detektiranje i sprječavanje upada te protumjere i otklanjanje posljedica nastalih zbog napada sprječavanja i odbijanja usluge.

5. Integritet usluga i sustava i kontrola dostupnosti

5.1. Dobavljač će: (a) provoditi procjene rizika sigurnosti i privatnosti najmanje jednom godišnje, (b) provoditi testiranje sigurnosti i procjenu ranjivosti, uključujući automatizirano sigurnosno skeniranje sustava i aplikacija i ručno etično hakiranje prije proizvodnog izdanja i jednom godišnje nakon toga što se tiče Usluga i Isporučivih materijala i jednom godišnje u pogledu Dobavljačevog Rukovanja Kyndryl-ovom Tehnologijom, (c) angažirati kvalificiranu neovisnu treću stranu za provođenje testiranja sigurnosti/proboja najmanje jednom godišnje sukladno Najboljim postupcima u industriji, gdje će takvo testiranje uključivati i automatizirano i ručno testiranje, (d) provoditi automatizirano upravljanje i rutinsku provjeru usklađenosti sa zahtjevima konfiguracije sigurnosti za svaku komponentu Usluga i Isporučivih materijala i u pogledu Dobavljačevog Rukovanja Kyndryl-ovom Tehnologijom, i (e) otkloniti identificirane ranjivosti ili neusklađenosti sa zahtjevima konfiguracije sigurnosti koje se temelje na povezanom riziku, iskoristivosti i utjecaju. Dobavljač će poduzeti razumne korake za izbjegavanje prekida Usluga prilikom testiranja, procjena, skeniranja i izvođenja aktivnosti ispravljanja grešaka. Na Kyndryl-ov zahtjev, Dobavljač će Kyndryl-u pružiti pisani sažetak Dobavljačevih tada najnovijih aktivnosti testiranja sigurnosti/proboja, gdje u izvještaju mora minimalno stajati naziv ponude pokrivene testiranje, broj sustava ili aplikacija u opsegu testiranja, datumi testiranja, metodologija korištena u testiranju te sažetak nalaza visoke razine.

5.2. Dobavljač će održavati politike i procedure namijenjene za upravljanje rizicima povezanima s primjenom promjena na Usluge ili Isporučive materijala ili na Rukovanje Kyndryl-ovom Tehnologijom. Prije implementiranja takve promjene, koja uključuje zahvaćene sustave, mreže i temeljne komponente, Dobavljač će u registriranom zahtjevu za promjenu dokumentirati: (a) opis razlog za promjenu, (b) detalje implementacije i raspored, (c) izjavu o riziku koja se odnosi na utjecaj na Usluge i Isporučive materijale, korisnike Usluga ili Kyndryl-ovih Materijala, (d) očekivani ishod, (e) plan vraćanja u prethodno stanje i (f) odobrenje ovlaštenih Dobavljačevih zaposlenika.

5.3. Dobavljač će održavati popis svih IT sredstava koja Dobavljač koristi za rad Usluga, pružanje Isporučivih materijala i Rukovanje Kyndryl-ovom Tehnologijom. Dobavljač će neprekidno nadgledati i upravljati stanjem (uključujući kapacitet) i dostupnost takvih IT sredstava, Usluga, Isporučivih materijala i Kyndryl-ove Tehnologije, uključujući temeljne komponente takvih sredstava, Usluga, Isporučivih materijala i Kyndryl-ove Tehnologije.

5.4. Dobavljač će izgraditi sve sustave koje koristi u razvoju ili u radu Usluga i Isporučivih materijala i za svoje Rukovanje Kyndryl-ovom Tehnologijom iz preddefiniranih slika sigurnosti sustava ili sigurnosnih osnova, koji zadovoljavaju Najbolje postupke u industriji kao što su sustavi mjerenja koje je definirao Center for Internet Security (CIS).

5.5. Bez ograničavanja Dobavljačevih odgovornosti ili Kyndryl-ovih prava temeljem ovog Transakcijskog dokumenta ili pridruženog osnovnog ugovora između strana u pogledu poslovnog kontinuiteta, Dobavljač će zasebno procijeniti svaku Uslugu i Isporučivi materijal i svaki IT sustav koji se koristi u Rukovanju Kyndryl-ovom Tehnologijom za poslovni i IT kontinuitet i zahtjeve obnavljanja od katastrofe sukladno dokumentiranim smjernicama za upravljanje rizikom. Dobavljač će osigurati da svaka takva Usluga, Isporučivi materijal i IT sustav ima u mjeri zajamčenoj takvom procjenom rizika, zasebno definirane, dokumentirane, održavane i godišnje potvrđene planove poslovnog i IT kontinuiteta i obnavljanja od katastrofe u skladu s Najboljim postupcima u industriji. Dobavljač će osigurati da su takvi planovi namijenjeni za pružanje određenih ciljeva vremena obnavljanja koji su navedeni u odjeljku 5.6 u nastavku.

5.6. Određeni ciljevi točke obnavljanja ("**RPO**")(engl. Recovery Point Objectives) i ciljevi vremena obnavljanja ("**RTO**") (engl. Recovery Time Objectives) u pogledu bilo koje Hostirane Usluge su: 24 satni RPO i 24 satni RTO; unatoč tome Dobavljač će u što kraćem roku pristati na bilo koje kraće trajanje RPO-a ili RTO-a na koje se Kyndryl obvezao prema Korisniku nakon Kyndryl-ove pisane obavijesti Dobavljaču o takvom kraćem trajanju RPO-a ili RTO-a (e-poruka se smatra pisanom obavijesti). Budući da se tiče svih ostalih Usluga koje Dobavljač pruža Kyndryl-u, Dobavljač će osigurati da su njegovi planovi poslovnog kontinuiteta i obnavljanja od katastrofe dizajnirani za

pružanje RPO-a i RTO-a takvi da Dobavljaču omogućuju daljnju potpunu sukladnost sa svim svojim obvezama prema Kyndryl-u temeljem Transakcijskog dokumenta i pridruženog osnovnog ugovora između strana kao i ovih Odredbi, uključujući obveze pravovremenog provođenja testiranja, pružanja podrške i održavanja.

5.7. Dobavljač će održavati mjere namijenjene procjeni, testiranju i primjeni zakrpa savjeta sigurnosti za Usluge i Isporučive materijale kao i za povezane sustave, mreže, aplikacije i temeljne komponente unutar opsega dotičnih Usluga i Isporučivih materijala te za sustave, mreže, aplikacije i temeljne komponente koje se koriste za Rukovanje Kyndryl-ovom Tehnologijom. Nakon utvrđivanja da je zakrpa savjeta sigurnosti primjenjiva i prikladna, Dobavljač će implementirati zakrpu sukladno dokumentiranoj ozbiljnosti i smjernicama procjene rizika. Dobavljačeva implementacija zakrpa savjeta sigurnosti predmet je njegove politike upravljanja promjenama.

5.8. Ako Kyndryl ima razumnu osnovu smatrati da hardver ili softver kojeg Dobavljač pruža Kyndryl-u može sadržavati intruzivne elemente poput špijunskog softvera (spyware), zlonamjernog softvera (malware) ili zlonamjernog koda (malicious code), Dobavljač će pravodobno surađivati s Kyndryl-om u istrazi i otklanjanju Kyndryl-ove zabrinutosti.

6. Pružanje usluge

6.1 Dobavljač će podržavati industrijski uobičajene metode udružene provjere identiteta za Kyndryl-ove ili Korisnikove korisničke račune, pri čemu će Dobavljač slijediti Najbolje postupke u industriji za provjeru identiteta takvih Kyndryl-ovih ili Korisnikovih korisničkih računa (kao putem Kyndryl-ovog centralno upravljanog višeparametarskog Single Sign-On-a (SSO), uz korištenje proizvoda OpenID Connect (OICD) ili Security Assertion Markup Languagea (SAML).

7. Podugovarači. Bez ograničavanja Dobavljačevih odgovornosti ili Kyndryl-ovih prava temeljem Transakcijskog dokumenta ili pridruženog osnovnog ugovora između strana u pogledu angažiranja podugovarača, Dobavljač će osigurati da svaki podugovarač koji obavlja posao za Dobavljača ima uspostavljene kontrole upravljanja sukladne zahtjevima i obvezama koje ove Odredbe nameću Dobavljaču

8. Fizički medij. Dobavljač će sigurno izbrisati fizički medij namijenjen ponovnoj upotrebi prije takve upotrebe, a uništit će fizički medij koji nije namijenjen ponovnoj upotrebi, u skladu s Najboljim postupcima u industriji za brisanje medija.

Članak IX Certifikati i izvještaji Hostiranih usluga

Ovaj članak se primjenjuje ako Dobavljač pruža Hostirane usluge Kyndryl-u.

1.1 Dobavljač će pribaviti sljedeće certifikate ili izvještaje unutar vremenskih okvira navedenih ispod:

Certifikati / Izvještaji	**Vremenski okvir**
Za Dobavljačeve Hostirane Usluge: Certifikat usklađenosti s ISO 27001, Informacijska tehnologija, Sigurnosne tehnike, Sustavi upravljanja sigurnošću informacija, s certifikatima koji se temelje na procjeni uglednog neovisnog revizora **ili** SOC 2 tip 2: Izvještaj uglednog neovisnog revizora koji prikazuje reviziju Dobavljačevih sustava, kontrola i operacija u skladu sa SOC 2 tip 2 (uključujući minimalno sigurnost, povjerljivost i dostupnost)	Dobavljač će pribaviti ISO 27001 certifikat u roku 120 dana od datuma stupanja na snagu ovog Transakcijskog dokumenta* ili datuma preuzimanja** i zatim će obnavljati certifikat na bazi procjene uglednog neovisnog revizora svakih 12 mjeseci nakon toga (svako obnavljanje odnosit će se na tada važeću verziju standarda) Dobavljač će pribaviti SOC 2 tip 2 izvještaj u roku 240 dana nakon stupanja na snagu Transakcijskog dokumenta* ili datuma preuzimanja** i zatim će pribaviti novi izvještaj uglednog neovisnog revizora koji prikazuje reviziju Dobavljačevih sustava, kontrola i operacija u skladu sa SOC 2 tip 2 (uključujući minimalno sigurnost, povjerljivost i dostupnost) svakih 6 mjeseci nakon toga * Ako od datuma stupanja na snagu Dobavljač pruža Hostiranu uslugu ** Datum kad Dobavljač preuzima obvezu pružanja Hostirane usluge

1.2 Ako Dobavljač pisano zatraži, a Kyndryl pisano odobri, Dobavljač može pribaviti certifikat ili izvještaj sadržajno ekvivalentan gore navedenima, uz razumijevanje da se vremenski okviri navedeni u tablici iznad primjenjuju jednako u pogledu sadržajno ekvivalentnog certifikata ili izvještaja.

1.3 Dobavljač će: (a) na zahtjev u što kraćem roku Kyndryl-u pružiti primjerak svakog certifikata i izvještaj koji je Dobavljač dužan pribaviti i (b) u što kraćem roku riješiti bilo koje slabosti unutarnje kontrole zabilježene tijekom SOC 2 ili sadržajno ekvivalentnih (ako ih Kyndryl odobri) revizija.

Članak X Suradnja, provjera i ispravljanje

Ovaj članak se primjenjuje ako Dobavljač pruža bilo koje Usluge ili Isporučive materijale Kyndryl-u.

1. Suradnja Dobavljača

1.1. Ako Kyndryl ima razloga za sumnju da je bilo koja Usluga ili Isporučivi materijal doprinio, doprinosi ili će doprinijeti bilo kojem problemu računalne sigurnosti, Dobavljač će razumno surađivati u Kyndryl-ovim ispitivanjima gleda takvih bojazni, uključujući pružanje pravovremenih i potpunih odgovora na zatražene informacije bilo putem dokumentacije, drugih evidencija, razgovora s odgovarajućim Dobavljačevim Osobljem ili slično.

1.2. Strane se slažu da će: (a) međusobno na zahtjev dostavljati takve dodatne informacije, (b) izvršavati i dostavljati jedna drugoj takve dodatne dokumente i (c) činiti druge radnje i stvari, sve što druga strana može razumno zatražiti u svrhu provođenja namjere ovih Odredbi i dokumenata na koje se upućuje u ovim Odredbama. Na primjer, ako Kyndryl zatraži, Dobavljač će pravodobno pružiti odredbe svojih pisanih ugovora s Podizvršiteljima obrade i podizvođačima, koje se odnose na privatnost i sigurnost, uključujući, tamo gdje to Dobavljač ima pravo učiniti, dodijelit će pristup samim ugovorima.

1.3. Ako Kyndryl zatraži, Dobavljač će pravodobno pružiti informacije o državama u kojima se proizvode, razvijaju ili na drugi način dobivaju Isporučivi materijali i njihove komponente.

2. Provjera (kako se koristi u nastavku, "Objekt" označava fizičku lokaciju na kojoj Dobavljač pruža hosting, obrađuje ili na drugi način pristupa Kyndryl-ovim Materijalima)

2.1. Dobavljač će održavati evidenciju u kojoj se revizijom može provjeriti usklađenost s ovim Odredbama

2.2. Kyndryl, sam ili s vanjskim revizorom, može uz pisanu obavijest Dobavljaču 30 dana unaprijed provjeriti Dobavljačevu sukladnost s ovim Odredbama, uključujući pristup bilo kojem Objektu ili Objektima u takve svrhe, iako Kyndryl neće pristupiti bilo kojem centru podataka u kojem Dobavljač Obrađuje Kyndryl-ove Podatke ako nema dobar razlog radi kojeg vjeruje da će time pružiti relevantne informacije. Dobavljač će surađivati u Kyndryl-ovoj provjeri, uključujući pružanje pravovremenih i potpunih odgovora na zatražene informacije bilo putem dokumentacije, drugih evidencija, razgovora s odgovarajućim Dobavljačevim osobljem ili sličnog. Dobavljač može pružiti dokaz o poštivanju odobrenog kodeksa ponašanja ili industrijskog certifikata ili na drugi način pružiti informacije Kyndryl-u kako bi dokazao usklađenost s ovim Odredbama za Kyndryl-ovo razmatranje.

2.3. Provjera se neće događati češće od jedanput u bilo kojem 12 mjesečnom periodu, osim ako: (a) Kyndryl provjerava Dobavljačevo ispravljanje problema koji su posljedica prethodne provjere tijekom 12 mjesečnog perioda ili (b) se pojavila Povreda sigurnosti i Kyndryl želi provjeriti poštivanje obveza relevantnih za tu povredu. U bilo kojem slučaju, Kyndryl će pružiti jednaku pisanu obavijest 30 dana unaprijed kako je navedeno u odjeljku 2.2 iznad, ali hitnost rješavanja Povrede sigurnosti može zahtijevati da Kyndryl provede provjeru ranije od 30 dana nakon pisane obavijesti.

2.4. Nadzorno tijelo ili drugi Voditelj obrade mogu ostvariti ista prava kao Kyndryl iz odjeljaka 2.2 i 2.3, uz razumijevanje da nadzorno tijelo može ostvariti bilo koja dodatna prava koja ima prema zakonu.

2.5. Ako Kyndryl ima razumnu osnovu koja daje zaključiti da Dobavljač ne poštuje bilo koju od ovih Odredbi (bilo da je osnova nastala iz provjere provedene na temelju ovih Odredbi ili na drugi način), tada će Dobavljač odmah ispraviti takvu neusklađenost.

3. Program protiv krivotvorenja

3.1. Ako Dobavljačevi Isporučivi materijali uključuju elektroničke komponente (npr. tvrde diskove, solid-state diskove (SSD), memoriju, središnje procesorske jedinice (CPU), logičke uređaje ili kablove), Dobavljač će održavati i slijediti dokumentirani program sprječavanja krivotvorenja kako bi prije svega spriječio da Dobavljač pruži krivotvorene komponente Kyndryl-u i drugo, kako bi odmah otkrio i ispravio u slučaju da Dobavljač zabunom pruži krivotvorene komponente Kyndryl-u. Dobavljač će nametnuti istu obvezu održavanja i praćenja programa sprječavanja krivotvorina svim svojim

dobavljačima od kojih nabavlja elektroničke komponente koje se ugrađuju u Isporučive materijale koje Dobavljač pruža Kyndryl-u.

4. Ispravljanje

4.1. Ako Dobavlja ne ispuni bilo koju od svojih obveza temeljem ovih Odredbi i takav propust uzrokuje Povredu sigurnosti, tada će Dobavljač ispraviti grešku u svom radu i otkloniti štetne utjecaje Povrede sigurnosti, a izvođenje i ispravljanje provodit će se uz Kyndryl-ove razumne upute i raspored. Međutim, ako do Povrede sigurnosti dođe zbog Dobavljačevog pružanja Hostiranih usluga za više zakupaca, pa posljedično utječe na mnoge Dobavljačeve korisnike uključujući Kyndryl, Dobavljač će, s obzirom na prirodu Povrede sigurnosti, pravovremeno i na odgovarajući način ispraviti grešku u svojoj izvedbi i otkloniti štetne učinke Povrede sigurnosti, pri čemu će se uzeti u obzir sve Kyndryl-ove napomene u vezi s takvim ispravkama i korektivnim mjerama.

4.2. Kyndryl će imati pravo sudjelovati u ispravljanju bilo koje Povrede sigurnosti na koju se upućuje u odjeljku 4.1 ako smatra da je to prikladno ili potrebno, a Dobavljač će biti odgovoran za svoje troškove i naknade u ispravljanju svoje izvedbe te za troškove i naknade ispravljanja kojima su se izložile strane u pogledu bilo koje takve Povrede sigurnosti.

4.3. Na primjer, troškovi i naknade za ispravljanje vezano uz Povredu sigurnosti mogu uključivati troškove i naknade za otkrivanje i istragu Povrede sigurnosti, utvrđivanje odgovornosti temeljem primjenjivih zakona i propisa, obavještavanje o povredi, uspostavljanje i održavanje pozivnih centara, pružanje usluga nadziranja i usluga vraćanja odobrenja, ponovno učitavanje podataka, ispravljanje grešaka proizvoda (uključujući kroz Izvorni kod ili drugi razvoj), zadržavanje trećih strana kao pomoć kod prethodno navedenih ili drugih relevantnih aktivnosti te ostale troškove i naknade neophodne za ispravljanje štetnih učinaka Povrede sigurnosti. Radi jasnoće, troškovi i naknade za ispravljanje neće uključivati Kyndryl-ov gubitak profita, posla, poslovne vrijednosti, prihoda, ugleda ili očekivanih ušteda.