

## ***Člen I: Poslovne kontaktne informacije***

Ta člena velja, če dobavitelj ali Kyndryl obdeluje PKI drugega.

1.1 Kyndryl in dobavitelj lahko obdelujeta PKI drugega povsod, kjer poslujeta v zvezi z dobaviteljevo dobavo storitev in elementov za dostavo.

1.2 Pogodbena stranka:

(a) ne bo uporabljala ali razkrivala PKI druge pogodbene stranke za noben drug namen (v pojasnilo: nobena pogodbeni stranka ne bo prodajala PKI druge stranke oziroma jih uporabljala ali razkrivala za kakršen koli trženjski namen brez predhodnega pisnega soglasja druge pogodbene stranke, in kjer je to zahtevano, brez predhodnega pisnega soglasja zadevnih oseb, na katere se nanašajo podatki), in

(b) bo ob prejetju pisne zahteve druge stranke nemudoma izbrisala, spremenila, popravila, vrnila, zagotovila informacije o obdelavi ali omejila obdelavo ali sprejela kateri koli drug razumno zahtevan ukrep v povezavi s PKI druge stranke, vedno ko pride do nepooblaščen uporabe osebnih podatkov in želi pogodbeni stranka prenehati obdelavo in izvesti sanacijo.

1.3 Pogodbene stranki ne vstopata v razmerje skupnega upravljavca glede poslovnih kontaktnih informacij druga druge in nobena določba transakcijskega dokumenta se ne razume ali interpretira kot znak kakršnega koli namena vzpostavitve razmerja skupnega upravljavca.

1.4 Izjava o zasebnosti družbe Kyndryl na naslovu <https://www.kyndryl.com/us/en/privacy> vsebuje dodatne podrobnosti o obdelavi PKI družbe Kyndryl.

1.5 Pogodbene stranki sta uvedli in bosta vzdrževali tehnične in organizacijske varnostne ukrepe za zaščito PKI druga druge pred izgubo, uničenjem, spreminjanjem, nenamernim ali nepooblaščenim razkritjem, nenamernim ali nepooblaščenim dostopom in nezakonito obdelavo.

1.6 Dobavitelj bo nemudoma (najpozneje v 48 urah) obvestil Kyndryl, ko bo izvedel za kakršno koli kršitev varnosti, ki vključuje PKI družbe Kyndryl. Dobavitelj bo poslal takšno obvestilo na e-naslov: [cyber.incidents@kyndryl.com](mailto:cyber.incidents@kyndryl.com). Dobavitelj bo družbi Kyndryl zagotovil razumno zahtevane informacije o taki kršitvi in statusu morebitnih dobaviteljevih dejavnosti za sanacijo in obnovo. Razumno zahtevane informacije lahko na primer vključujejo dnevnik, ki prikazujejo privilegiran, skrbniški in drug dostop do naprav, sistemov ali aplikacij, forenzične slike naprav, sistemov ali aplikacij in druge podobne elemente, in sicer do mere, ki je primerna kršitvi ali dobaviteljevim dejavnostim za sanacijo in obnovitev.

1.7 Če dobavitelj zgolj obdeluje PKI družbe Kyndryl in nima dostopa do nobenih drugih podatkov ali materialov kakršne koli vrste ali do nobenega poslovnega sistema družbe Kyndryl, sta ta člen in člen X (Sodelovanje, preverjanje in sanacija) edina člena, ki veljata za takšno obdelavo.

## **Člen II: Tehnični in organizacijski ukrepi, varnost podatkov**

Ta člen velja, če dobavitelj obdeluje podatke družbe Kyndryl, ki niso PKI družbe Kyndryl. Dobavitelj bo pri zagotavljanju vseh storitev in elementov za dostavo ravnal skladno z zahtevami tega člena in s tem zaščitil podatke družbe Kyndryl pred izgubo, uničenjem, spreminjanjem, nenamernim ali nepooblaščenim razkritjem, nenamernim ali nepooblaščenim dostopom in nezakonitimi oblikami obdelave. Zahteve tega člena veljajo za vse informacijskotehnološke aplikacije, platforme in infrastrukturo, ki jih dobavitelj uporablja ali upravlja pri zagotavljanju elementov za dostavo in storitev, vključno z vsemi okolji za razvoj, preizkušanje, gostovanje, podporo, delovanje in podatkovne centre.

### **1. Uporaba podatkov**

1.1 Dobavitelj brez predhodnega pisnega soglasja družbe Kyndryl podatkom družbe Kyndryl ne sme dodajati ali prilagati nobenih drugih informacij ali podatkov, vključno z osebnimi podatki, in dobavitelj podatkov družbe Kyndryl v nobeni obliki, bodisi združeni bodisi drugačni, ne sme uporabljati za noben namen razen za zagotavljanje storitev in elementov za dostavo (dobavitelj na primer ne sme uporabljati ali ponovno uporabljati podatkov družbe Kyndryl za ocenjevanje ali povečevanje uspešnosti svojih ponudb, za raziskovanje in razvoj pri ustvarjanju novih ponudb ali za ustvarjanje poročil glede svojih ponudb). Dobavitelj ne sme prodajati podatkov družbe Kyndryl, razen če je to izrecno dovoljeno v transakcijskem dokumentu.

1.2 Dobavitelj v elemente za dostavo ali kot del storitev ne bo vdeloval nobenih tehnologij za spletno spremljanje (takšne tehnologije vključujejo HTML5, lokalno shranjevanje, oznake ali žetone tretjih oseb in spletne signale), razen če je to izrecno dovoljeno v transakcijskem dokumentu.

### **2. Zahteve tretjih oseb in zaupnost**

2.1 Dobavitelj ne bo razkril podatkov družbe Kyndryl nobeni tretji osebi, razen če Kyndryl to vnaprej pisno odobri. Če vladni organ, vključno s katerim koli regulatorjem, zahteva dostop do podatkov družbe Kyndryl (če na primer ameriški vladni organ dobavitelju vroči odredbo o nacionalni varnosti za pridobitev podatkov družbe Kyndryl) ali če razkritje podatkov družbe Kyndryl zahteva zakonodaja, bo dobavitelj pisno obvestil družbo Kyndryl o takšni zahtevi in zagotovil družbi Kyndryl razumno priložnost, da izpodbija kakršno koli razkritje (kjer zakonodaja prepoveduje obveščanje, bo dobavitelj sprejel ukrepe, za katere razumno meni, da so ustrezni za izpodbijanje prepovedi in razkritja podatkov družbe Kyndryl prek sodnega postopka ali na drug način).

2.2 Dobavitelj družbi Kyndryl zagotavlja: (a) da bodo imeli dostop do podatkov družbe Kyndryl samo tisti njegovi uslužbenci, ki tak dostop potrebujejo za zagotavljanje storitev ali elementov za dostavo, in še to samo v meri, ki je potrebna za zagotavljanje teh storitev in elementov za dostavo; in (b) da je zavezal svoje zaposlene z obveznostmi zaupnosti, ki od njih zahtevajo, da podatke družbe Kyndryl uporabljajo in razkrivajo samo tako, kot to dovoljujejo te določbe.

### **3. Vračilo ali izbris podatkov družbe Kyndryl**

3.1 Dobavitelj bo, če se Kyndryl tako odloči, ob prenehanju ali poteku transakcijskega dokumenta oziroma prej na zahtevo družbe Kyndryl bodisi izbrisal podatke družbe Kyndryl bodisi jih vrnil družbi Kyndryl. Če bo Kyndryl zahteval izbris, bo dobavitelj v skladu z najboljšimi panožnimi praksami podatke spremenil tako, da jih ne bo mogoče prebrati, ponovno sestaviti ali rekonstruirati, in družbi Kyndryl potrdil izbris. Če bo Kyndryl zahteval vračilo svojih podatkov, bo dobavitelj to naredil v skladu z razumnim časovnim razporedom družbe Kyndryl in po njenih razumnih pisnih navodilih.

### **Člen III: Zasebnost**

Ta člen velja, če dobavitelj obdeluje osebne podatke družbe Kyndryl.

#### **1. Obdelava podatkov**

1.1 Kyndryl imenuje dobavitelja za obdelovalca, ki osebne podatke družbe Kyndryl obdeluje izključno za namen zagotavljanja elementov za dostavo in storitev v skladu z navodili družbe Kyndryl, vključno s tistimi, ki jih vsebujejo te določbe, transakcijski dokument in povezana osnovna pogodba med pogodbenima strankama. Če dobavitelj ne upošteva katerega od navodil, lahko Kyndryl s pisnim obvestilom odpove del storitev, na katere to vpliva. Če dobavitelj meni, da katero od navodil krši zakon o varstvu podatkov, bo družbo Kyndryl o tem obvestil takoj in v časovnem okviru, ki ga zahteva zakon. Če dobavitelj ne spoštuje katere koli od svojih obveznosti iz teh določb in to nespoštovanje povzroči nepooblaščen uporabo osebnih podatkov, ali na splošno v katerem koli primeru nepooblaščen uporabe osebnih podatkov, lahko Kyndryl ustavi obdelavo in odpravi napako ter sanira škodljive učinke nepooblaščen uporabe, pri takšnem izvajanju in sanaciji pa upošteva razumna navodila in časovni okvir družbe Kyndryl.

1.2 Dobavitelj bo ravnal skladno z vsemi zakoni o varstvu podatkov, ki veljajo za storitve in elemente za dostavo.

1.3 Dodatek k transakcijskemu dokumentu ali sam transakcijski dokument v zvezi s podatki družbe Kyndryl izpostavlja naslednje:

- (a) kategorije posameznikov, na katere se nanašajo osebni podatki;
- (b) vrste osebnih podatkov družbe Kyndryl;
- (c) dejanja in dejavnosti obdelave podatkov;
- (d) trajanje in pogostost obdelave;
- (e) seznam podobdelovalcev.

#### **2. Tehnični in organizacijski ukrepi**

2.1 Dobavitelj bo uvedel in vzdrževal tehnične in organizacijske ukrepe, ki so opredeljeni v členu II (Tehnični in organizacijski ukrepi, varnost podatkov) in členu VIII (Tehnični in organizacijski ukrepi, splošna varnost), s čimer bo zagotovil raven varnosti, ki je primerna za tveganje, ki ga predstavljajo njegove storitve in elementi za dostavo. Dobavitelj potrjuje in razume omejitve v členu II, tem členu III in členu VIII ter bo ravnal skladno z njimi.

#### **3. Pravice in zahteve posameznikov, na katere se nanašajo osebni podatki**

3.1 Dobavitelj bo takoj obvestil družbo Kyndryl (v skladu s časovnim razporedom, ki družbi Kyndryl in morebitnim drugim upravljavcem omogoča izpolnitev njihovih pravnih obveznosti) o kakršni koli zahtevi osebe, na katero se nanašajo podatki, glede uveljavljanja njenih pravic (npr. popravek, izbris ali blokiranje podatkov) glede osebnih podatkov družbe Kyndryl. Dobavitelj lahko osebo, na katero se nanašajo podatki in ki vloži takšno zahtevo, tudi takoj usmeri k družbi Kyndryl. Dobavitelj ne bo odgovarjal na nobene zahteve oseb, na katere se nanašajo osebni podatki, razen če to zahteva zakon ali Kyndryl to zahteva v pisni obliki.

3.2 Če mora Kyndryl zagotoviti informacije glede svojih osebnih podatkov drugim upravljavcem ali drugim tretjim osebam (npr. osebam, na katere se nanašajo podatki, ali regulatorjem), bo dobavitelj družbi Kyndryl pomagal tako, da bo zagotovil informacije in sprejel druge razumne ukrepe, ki jih bo zahteval Kyndryl, v časovnem okviru, ki družbi Kyndryl omogoča, da se pravočasno odzove takšnim drugim upravljavcem ali tretjim osebam.

## 4. Podobdelovalci

4.1 Dobavitelj bo družbi Kyndryl poslal vnaprejšnje pisno obvestilo, preden bo dodal novega podobdelovalca ali razširil obseg obdelave z obstoječim podobdelovalcem, v tem pisnem obvestilu pa bo navedeno ime podobdelovalca in opisan bo nov ali razširjeni obseg obdelave. Kyndryl lahko na podlagi utemeljenih razlogov kadar koli nasprotuje vsakemu takšnemu novemu podobdelovalcu ali razširjenemu obsegu; v tem primeru bosta pogodbeni stranki v dobri veri sodelovali pri obravnavi nasprotovanja družbe Kyndryl. V skladu s pravico družbe Kyndryl do takšnega nasprotovanja lahko dobavitelj imenuje novega podobdelovalca ali razširi obseg obdelave obstoječega podobdelovalca, če Kyndryl v 30 dneh od prejema dobaviteljevega pisnega obvestila temu ne nasprotuje.

4.2 Dobavitelj bo obveznosti glede zaščite podatkov, varnosti in certifikatov, opredeljene v teh določbah, naložil vsakemu odobrenemu podobdelovalcu, preden bo ta obdelal kakršne koli podatke družbe Kyndryl. Dobavitelj v celoti odgovarja družbi Kyndryl za izvajanje obveznosti vsakega podobdelovalca.

## 5. Čezmejna obdelava podatkov

Kot se uporablja v nadaljevanju:

**Ustrezna država** pomeni državo, ki zagotavlja ustrezno raven varstva podatkov v zvezi z zadevnim prenosom v skladu z veljavnimi zakoni o varstvu podatkov ali odločitvami regulatorjev.

**Uvoznik podatkov** pomeni bodisi obdelovalca bodisi podobdelovalca, ki nima sedeža podjetja v ustrezni državi.

**Standardne pogodbene klavzule EU** (»standardne pogodbene klavzule EU«) pomenijo standardne pogodbene klavzule EU (Odločba Komisije 2021/914) z uporabljenimi neobveznimi klavzulami, razen možnosti 1 klavzule 9(a) in možnosti 2 klavzule 17, kot je uradno objavljeno na spletni strani [https://commission.europa.eu/publications/standard-contractual-clauses-international-transfers\\_en](https://commission.europa.eu/publications/standard-contractual-clauses-international-transfers_en).

**Srbske standardne pogodbene klavzule** (»srbske standardne pogodbene klavzule«) pomenijo srbske standardne pogodbene klavzule, kot jih je sprejel »srbski komisar za informacije javnega pomena in varstvo osebnih podatkov« in so objavljene na naslovu <https://www.poverenik.rs/images/stories/dokumentacija-nova/podzakonski-akti/Klavzulelat.docx>.

**Standardne pogodbene klavzule** (»standardne pogodbene klavzule«) pomenijo pogodbene klavzule, ki jih zahtevajo veljavni zakoni o varstvu podatkov za prenos osebnih podatkov obdelovalcem, ki nimajo sedeža podjetja v ustreznih državah.

**Dopolnilo Združenega kraljestva o notranjem prenosu podatkov k standardnim pogodbenim klavzulam Evropske komisije** (»dopolnilo ZK«) pomeni dopolnilo Združenega kraljestva o notranjem prenosu podatkov k standardnim pogodbenim klavzulam Evropske komisije, kot so uradno objavljene na naslovu <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-Transfer-agreement-and-guidance/>.

**Švicarsko dopolnilo k standardnim pogodbenim klavzulam Komisije EU** (»Švicarsko dopolnilo«) pomeni pogodbene klavzule k standardnim pogodbenim klavzulam Komisije EU, ki se uveljavljajo v skladu z odločitvijo švicarskega organa za varstvo podatkov (»**FDPIC**«) in v skladu s švicarskim zveznim zakonom o varstvu podatkov (»**FADP**«).

5.1 Dobavitelj brez predhodnega pisnega soglasja družbe Kyndryl ne bo čezmejno prenašal ali razkrival (vključno z oddaljenim dostopom) kakršnih koli osebnih podatkov družbe Kyndryl. Če Kyndryl zagotovi takšno soglasje, bosta pogodbeni stranki v sodelovanju zagotovili skladnost z veljavnimi zakoni o varstvu podatkov. Če ti zakoni zahtevajo standardne pogodbene klavzule, jih bo dobavitelj na zahtevo družbe Kyndryl takoj sklenil.

## 5.2 V zvezi s standardnimi pogodbenimi klavzulami EU:

(a) Če dobavitelj nima sedeža podjetja v ustrezni državi: dobavitelj s tem dokumentom z družbo Kyndryl sklepa standardne pogodbene klavzule EU kot uvoznik podatkov in bo z vsakim odobrenim podobdelovalcem sklenil pisne pogodbe v skladu s členom 9 standardnih pogodbenih klavzul EU, družbi Kyndryl pa bo na zahtevo zagotovil izvode teh pogodb.

(i) Modul 1 standardnih pogodbenih klavzul EU ne velja, razen če se pogodbeni stranki v pisni obliki dogovorita drugače.

(ii) Modul 2 standardnih pogodbenih klavzul EU velja tam, kjer je Kyndryl upravljavec, modul 3 pa tam, kjer je Kyndryl obdelovalec. Če v skladu s klavzulo 13 standardnih pogodbenih klavzul EU velja modul 2 ali 3, se pogodbeni stranki strinjata, (1) da bo standardne pogodbene klavzule EU urejala zakonodaja države članice EU, v kateri je pristojni nadzorni organ, in (2) da se bodo morebitni spori, ki izhajajo iz standardnih pogodbenih klavzul EU, reševali na sodiščih države članice EU, v kateri je pristojni nadzorni organ. Če takšna zakonodaja pod točko (1) ne dovoljuje pravic zunanjega upravičenca, potem standardne pogodbene klavzule EU ureja zakonodaja Nizozemske, vsi spori, ki izhajajo iz standardnih pogodbenih klavzul EU pod točko (2), pa se bodo reševali na sodišču v Amsterdamu na Nizozemskem.

(b) Če imata obe pogodbeni stranki, dobavitelj in Kyndryl, sedež podjetja v ustrezni državi, bo dobavitelj deloval kot uvoznik podatkov in bo z vsakim odobrenim podobdelovalcem, ki nima sedeža podjetja v ustrezni državi, sklenil standardne pogodbene klavzule EU. Dobavitelj bo izvedel zahtevano oceno vpliva prenosa (OVP) in družbo Kyndryl brez nepotrebnega odlašanja obvestil o (1) morebitni potrebi za vpeljavo dodatnih ukrepov in (2) uveljavljenih ukrepih. Na zahtevo bo dobavitelj posredoval rezultate OVP in katere koli informacije, potrebne za razumevanje in ovrednotenje rezultatov, družbi Kyndryl. Če se Kyndryl ne strinja z rezultati OVP dobaviteljev ali z uveljavljenimi dodatnimi ukrepi, bosta Kyndryl in dobavitelj skupaj poiskala sprejemljivo rešitev. Kyndryl si pridržuje pravico, da brez nadomestila prekine ali odpove dobaviteljeve storitve. V izogib dvomu: to ne odvezuje dobaviteljevih podobdelovalcev obveznosti, da postanejo pogodbeni stranka standardnih pogodbenih klavzul EU z družbo Kyndryl ali njenimi naročniki, kot je opisano v spodnjem razdelku 5.2 (d).

(c) Če ima dobavitelj sedež v Evropskem gospodarskem prostoru in je Kyndryl upravljavec, za katerega ne velja Splošna uredba o varstvu podatkov 2016/679, potem velja modul 4 standardnih pogodbenih klavzul EU, dobavitelj pa s tem dokumentom z družbo Kyndryl sklepa standardne pogodbene klavzule EU. Če velja modul 4 standardnih pogodbenih klavzul EU, se pogodbeni stranki strinjata, da bo standardne pogodbene klavzule EU urejala zakonodaja Nizozemske, vsi spori, ki izhajajo iz standardnih pogodbenih klavzul EU, pa se bodo reševali na sodišču v Amsterdamu na Nizozemskem.

(d) Če drugi upravljavci, kot so stranke ali povezane družbe, zahtevajo, da postanejo pogodbeni stranka standardnih pogodbenih klavzul EU v skladu s »klavzulo o umeščanju« v klavzuli 7, se dobavitelj s tem dokumentom strinja s katero koli takšno zahtevo.

(e) Tehnične in organizacijske ukrepe, ki so zahtevani za izpolnitev aneksa II standardnih pogodbenih klavzul EU, lahko najdete v teh določbah, samem transakcijskem dokumentu in povezani osnovni pogodbi med pogodbenima strankama.

(f) V primeru kakršnega koli navzkrižja med standardnimi pogodbenimi klavzulami EU in temi določbami prevladajo standardne pogodbene klavzule EU.

### 5.3 V zvezi z Dopolnilom(-i) ZK:

- (a) Če dobavitelj nima sedeža podjetja v ustrezni državi: (i) dobavitelj s tem dokumentom sklepa z družbo Kyndryl Dopolnilo/-a ZK kot uvoznik, s čimer se dopolnijo standardne pogodbene klavzule EU, kot so določene zgoraj (če je ustrezno, odvisno od okoliščin dejavnosti obdelave), in (ii) dobavitelj bo sklenil pisne pogodbe z vsakim odobrenim podobdelovalcem, družbi Kyndryl pa bo na zahtevo zagotovil izvode teh pogodb.
- (b) Če ima dobavitelj sedež podjetja v ustrezni državi in je Kyndryl upravljavec, za katerega ne velja Splošna uredba o varstvu podatkov ZK (kot je vključena v pravo ZK v skladu z zakonom o izstopu ZK iz Evropske unije iz leta 2018 (European Union (Withdrawal) Act 2018)), potem dobavitelj s tem dokumentom sklepa z družbo Kyndryl Dopolnilo/-a ZK kot izvoznik, s čimer se dopolnijo standardne pogodbene klavzule EU, kot so navedene v zgornjem razdelku 5.2(b).
- (c) Če drugi upravljavci, kot so naročniki ali povezana podjetja, zahtevajo, da postanejo pogodbeni stranka pri Dopolnilu/-ih ZK, se dobavitelj s tem dokumentom strinja s takšno zahtevo.
- (d) Informacije dodatka (kot so navedene v 3. razpredelnici) v Dopolnilu/-ih ZK je mogoče najti v veljavnih standardnih pogodbenih klavzulah EU, teh določilih, samem transakcijskem dokumentu in v povezanih osnovnih pogodbah med pogodbenimi strankami. Niti Kyndryl niti dobavitelj ne more prekiniti Dopolnil/-a ZK, ko se Dopolnilo ZK spremeni.
- (e) V primeru kakršnega koli navzkrižja med Dopolnilom/-i ZK in temi določbami prevlada/-jo Dopolnilo/-a ZK.

### 5.4 V zvezi s srbskimi standardnimi pogodbenimi klavzulami:

- (a) Če dobavitelj nima sedeža podjetja v ustrezni državi: (i) dobavitelj s tem dokumentom z družbo Kyndryl sklepa srbske standardne pogodbene klavzule v svojem imenu kot obdelovalec; in (ii) dobavitelj bo v skladu s členom 8 srbskih standardnih pogodbenih klavzul sklenil pisne pogodbe z vsakim odobrenim podobdelovalcem, družbi Kyndryl pa bo na zahtevo posredoval izvode teh pogodb.
- (b) Če ima dobavitelj sedež podjetja v ustrezni državi, dobavitelj s tem dokumentom z družbo Kyndryl sklepa srbske standardne pogodbene klavzule v imenu vsakega podobdelovalca, ki se nahaja v državi, v kateri ni ustreznega varstva. Če dobavitelj za katerega koli takšnega podobdelovalca tega ne more narediti, bo družbi Kyndryl v podpis posredoval srbske standardne pogodbene klavzule, ki jih podpiše ta podobdelovalec, in sicer preden podobdelovalcu dovoli obdelavo kakršnih koli osebnih podatkov družbe Kyndryl.
- (c) Srbske standardne pogodbene klavzule med družbo Kyndryl in dobaviteljem bodo služile bodisi kot srbske standardne pogodbene klavzule med upravljavcem in obdelovalcem bodisi kot obojestransko podpisana pogodba med »obdelovalcem« in »podobdelovalcem«, kot bodo narekovala dejstva. V primeru kakršnega koli navzkrižja med srbskimi standardnimi pogodbenimi klavzulami in temi določbami prevladajo srbske standardne pogodbene klavzule.
- (d) Informacije, potrebne za izpolnitev dodatkov od 1 do 8 srbskih standardnih pogodbenih klavzul za namene upravljanja prenosa osebnih podatkov v državo, v kateri ni ustreznega varstva, lahko najdete v teh pogojih in v dodatku k transakcijskemu dokumentu oziroma v samem transakcijskem dokumentu.

### 5.5 V zvezi s Švicarskim/-i dopolnilom/-i:

- (a) Če in v obsegu, v katerem za prenos osebnih podatkov družbe Kyndryl v skladu z razdelkom 5.1 velja švicarski zvezni zakon o varstvu podatkov (»FADP«), prenos urejajo standardne pogodbene klavzule EU, dogovorjene v razdelku 5.2 teh pogojev, z naslednjimi spremembami, tako da se sprejme standard GDPR za

švicarske osebne podatke:

- sklicevanja na Splošno uredbo o varstvu podatkov (»GDPR«) se razumejo tudi kot sklicevanja na enakovredne določbe FADP;
- švicarska zvezna informacijska komisija za varstvo podatkov je pristojni nadzorni organ v skladu s klavzulo 13 in aneksom I.C standardnih pogodbenih klavzul EU;
- švicarsko pravo kot pravo, ki se uporablja, če za prenos podatkov velja izključno FADP, in
- izraz »država članica« v klavzuli 18 standardnih pogodbenih klavzul EU vključi Švico, da se posameznikom, na katere se nanašajo osebni podatki, omogoči uveljavljanje pravic v kraju njihovega običajnega prebivališča.

(b) V izogib dvomu je treba poudariti, da noben od prej navedenih ukrepov ni namenjen temu, da bi kakor koli zmanjšal raven varstva podatkov, ki jo zagotavljajo standardne pogodbene klavzule EU, temveč le temu, da bi to raven varstva razširil na švicarske posameznike, na katere se nanašajo osebni podatki. Če to ne velja in v obsegu, v katerem to ne velja, prevladajo standardne pogodbene klavzule EU.

## **6. Pomoč in evidence**

6.1 Ob upoštevanju narave obdelave bo dobavitelj pomagal družbi Kyndryl tako, da bo imel vzpostavljene ustrezne tehnične in organizacijske ukrepe, s katerimi bo izpolnil obveznosti, povezane z zahtevami in pravicami oseb, na katere se nanašajo podatki. Dobavitelj bo družbi Kyndryl pomagal tudi pri zagotavljanju skladnosti z obveznostmi, povezanimi z varnostjo obdelave, obveščanjem in sporočanjem kršitve varnosti ter ustvarjanju ocen vpliva na varstvo podatkov, vključno s predhodnim posvetovanjem z odgovornim regulatorjem, če bo to zahtevano, pri čemer bodo upoštevane informacije, ki so mu na voljo.

6.2 Dobavitelj bo vzdrževal aktualno evidenco imen in kontaktnih podatkov vsakega od podobdelovalcev, vključno s predstavnikom in uradno osebo za varstvo podatkov podobdelovalca. Dobavitelj bo na zahtevo to evidenco zagotovil družbi Kyndryl v skladu s časovnim razporedom, ki bo družbi Kyndryl omogočal, da se bo pravočasno odzvala na kakršno koli zahtevo naročnika ali druge tretje osebe.

## **Člen IV: Tehnični in organizacijski ukrepi, varnost kode**

Ta člen velja, če lahko dobavitelj dostopa do izvorne kode družbe Kyndryl. Dobavitelj bo ravnal skladno z zahtevami tega člena in s tem zaščitil izvorno kodo Kyndryl pred izgubo, uničenjem, spreminjanjem, nenamernim ali nepooblaščenim razkritjem, nenamernim ali nepooblaščenim dostopom in nezakonitimi oblikami obravnavanja. Zahteve tega člena veljajo za vse informacijskotehnološke aplikacije, platforme in infrastrukturo, ki jih dobavitelj uporablja ali upravlja pri zagotavljanju elementov za dostavo in storitev ter pri obravnavanju tehnologije družbe Kyndryl, vključno z vsemi okolji za razvoj, preizkušanje, gostovanje, podporo, delovanje in podatkovne centre.

### **1. Zahteve glede varnosti**

Kot se uporablja v nadaljevanju:

**prepovedana država** pomeni katero koli državo: (a) ki jo je ameriška vlada določila kot tujega sovražnika v okviru izvršne uredbe z dne 15. maja 2019 o varovanju informacijske in komunikacijske tehnologije in dobavne verige storitev, (b) ki je navedena na seznamu v skladu z razdelkom 1654 ameriškega zakona o nacionalni obrambi iz leta 2019 ali (c) ki je v transakcijskem dokumentu določena kot »prepovedana država«.

1.1 Dobavitelj ne bo distribuiral ali deponiral nobene izvorne kode družbe Kyndryl v korist katere koli tretje osebe.

1.2 Dobavitelj ne bo dovolil, da bi se katera koli izvorna koda družbe Kyndryl nahajala v strežnikih v prepovedani državi. Dobavitelj ne bo dovolil nikomur, vključno svojemu osebju, ki se nahaja v prepovedani državi ali je na obisku v prepovedani državi (v času trajanja takšnega obiska), da bi iz kakršnega koli razloga dostopal do katere koli izvorne kode družbe Kyndryl ali jo uporabljal, ne glede na to, kje na svetu se ta izvorna koda družbe Kyndryl nahaja, in ne bo dovolil nobenega razvoja, preizkušanja ali drugega dela v prepovedani državi, ki bi zahtevalo takšen dostop ali uporabo.

1.3 Dobavitelj ne bo prestavljal ali distribuiral izvorne kode družbe Kyndryl v nobeno pristojnost, kjer zakonodaja ali interpretacija zakonodaje zahteva razkritje izvorne kode kateri koli tretji osebi. Če pride v pristojnosti, v kateri se nahaja izvorna koda družbe Kyndryl, do spremembe zakonodaje ali interpretacije zakonodaje, ki bi od dobavitelja lahko zahtevala razkritje takšne izvorne kode tretji osebi, bo dobavitelj nemudoma uničil ali nemudoma odstranil takšno izvorno kodo družbe Kyndryl iz takšne pristojnosti, in ne bo v takšno sodno pristojnost poslal nobene dodatne izvorne kode družbe Kyndryl, če bo takšna zakonodaja ali interpretacija zakonodaje ostala v veljavi.

1.4 Dobavitelj ne bo neposredno ali posredno sprejel nobenega ukrepa, vključno s sklenitvijo kakršne koli pogodbe, ki bi povzročil, da bi moral dobavitelj, Kyndryl ali katera koli tretja oseba sprejeti obveznost o razkritju informacij v okviru razdelka 1654 ali 1655 ameriškega zakona o nacionalni obrambi iz leta 2019. V pojasnilo: dobavitelju brez predhodnega pisnega soglasja družbe Kyndryl ni dovoljeno razkriti izvorne kode družbe Kyndryl nobeni tretji osebi v nobenih okoliščinah, razen če je to izrecno dovoljeno v transakcijskem dokumentu ali povezani osnovni pogodbi med pogodbenima strankama.

1.5 Če Kyndryl obvesti dobavitelja ali če tretja oseba obvesti katero koli od pogodbenih strank, da: (a) dobavitelj dovoli prenos izvorne kode družbe Kyndryl v prepovedano državo ali katero koli pristojnost, ki je predmet zgornjega razdelka 1.3, (b) je dobavitelj na drugačen način izdal, uporabljal izvorno kodo družbe Kyndryl ali dostopal do nje na način, ki ga transakcijski dokument ali povezana osnovna ali druga pogodba med pogodbenima strankama ne dovoljuje, ali (c) je dobavitelj kršil zgornji razdelek 1.4, potem brez omejevanja pravic družbe Kyndryl do obravnave takšne neskladnosti po pravni poti ali po načelih pravičnosti ali v okviru transakcijskega dokumenta ali povezane osnovne ali druge pogodbe med pogodbenima strankama velja naslednje: (i) če je takšno obvestilo poslano dobavitelju, ga bo dobavitelj takoj posredoval družbi Kyndryl; (ii) dobavitelj bo po razumnih navodilih družbe Kyndryl preiskal in saniral zadevo v skladu s časovnim razporedom, ki ga razumno določi Kyndryl (po posvetu z dobaviteljem).

1.6 Če Kyndryl razumno verjame, da so morda potrebne spremembe dobaviteljevih pravilnikov, postopkov, nadzorov ali praks v zvezi z dostopom do izvorne kode zaradi obravnavanja kibernetске varnosti, kraje intelektualne lastnine oziroma podobnih ali povezanih tveganj (vključno s tveganjem, da bo brez takšnih



sprememb družbi Kyndryl prepovedana prodaja določenim naročnikom ali na določene trge oziroma drugače ne bo mogel izpolniti naročnikovih zahtev glede varnosti ali dobavne verige), lahko Kyndryl stopi v stik z dobaviteljem zaradi pogovora o potrebnih ukrepih za obravnavanje takšnih tveganj, vključno s spremembami takšnih pravilnikov, postopkov, nadzorov ali praks. Dobavitelj bo na zahtevo družbe Kyndryl sodeloval z njo pri ocenjevanju potrebe po takšnih spremembah in pri uvajanju ustreznih in medsebojno dogovorjenih sprememb.

## **Člen V: Varen razvoj**

Ta člen velja, če bo dobavitelj zagotovil svojo izvorno kodo ali izvorno kodo tretje osebe oziroma programsko opremo na mestu uporabe družbi Kyndryl oziroma bodo kateri koli dobaviteljevi elementi za dostavo ali storitve zagotovljeni naročniku družbe Kyndryl kot del izdelka ali storitve družbe Kyndryl.

### **1. Varnostna pripravljenost**

1.1 Dobavitelj bo sodeloval pri notranjih postopkih družbe Kyndryl za ocenjevanje varnostne pripravljenosti izdelkov in storitev družbe Kyndryl, ki so odvisni od katerih koli dobaviteljevih elementov za dostavo, vključno s pravočasnim in celovitim odzivanjem na zahteve za informacije v obliki dokumentov, drugih zapisov, pogovorov z ustreznim dobaviteljevim osebjem in podobnega.

### **2. Varen razvoj**

2.1 Ta razdelek 2 velja samo v primeru, ko dobavitelj družbi Kyndryl zagotavlja programsko opremo na mestu uporabe.

2.2 Dobavitelj je uvedel in bo skozi celotno obdobje trajanja transakcijskega dokumenta v skladu z najboljšimi panožnimi praksami vzdrževal varnostne pravilnike, postopke in kontrole za omrežja, platforme, sisteme, aplikacije, naprave, fizično infrastrukturo, odzivanje na incidente ter osebje, ki so potrebni za zaščito: (a) razvoja, gradnje, preizkušanja, operacijskih sistemov in okolij, ki jih dobavitelj ali katera koli tretja oseba, ki jo najame dobavitelj, uporablja, upravlja ali se drugače zanaša nanje v zvezi z elementi za dostavo, in (b) vse izvorne kode elementov za dostavo pred izgubo, nezakonitimi oblikami rokovanja ter nepooblaščenim dostopom, razkritjem ali spreminjanjem.

### **3. Certifikat ISO 20243**

3.1 Ta razdelek 3 velja samo v primeru, če bodo kateri koli dobaviteljevi elementi za dostavo ali storitve zagotovljeni naročniku družbe Kyndryl kot del izdelka ali storitve družbe Kyndryl.

3.2 Dobavitelj bo pridobil certifikat o skladnosti s standardom ISO 20243, Informacijska tehnologija – Open Trusted Technology Provider™ Standard (O-TTPS) – Zmanjševanje zlonamerno okuženih in ponarejenih izdelkov (bodisi certifikat na osnovi samoocene bodisi certifikat na osnovi ocene uglednega neodvisnega revizorja). Če dobavitelj namesto tega pisno zaprosi Kyndryl, ta pa to pisno odobri, bo dobavitelj pridobil certifikat o skladnosti, ki je v bistvenih značilnostih enakovreden panožnim standardom, ki obravnava varen razvoj in prakse glede dobavne verige (bodisi certifikat na osnovi samoocene bodisi certifikat na osnovi ocene uglednega neodvisnega revizorja, če in kot ga odobri Kyndryl).

3.3 Dobavitelj bo pridobil certifikat o skladnosti s standardom ISO 20243 ali s panožnim standardom, ki je glede bistvenih značilnosti enakovreden (če to pisno odobri Kyndryl) v največ 180 dneh po datumu veljavnosti transakcijskega dokumenta in nato podaljšal certifikat vsakih 12 mesecev zatem (vsako podaljšanje je glede na trenutno različico takrat veljavnega standarda, npr. ISO 20243 ali, kjer to v pisni obliki potrdi Kyndryl, v bistvenih značilnostih enakovrednega panožnega standarda, ki obravnava prakse varnega razvoja in dobavne verige).

3.4 Dobavitelj bo na zahtevo družbi Kyndryl takoj zagotovil kopijo certifikatov, ki jih mora pridobiti v skladu z zgornjima razdelkoma 2.1 in 2.2.

#### 4. Varnostne ranljivosti

Kot se uporablja v nadaljevanju:

**Popravek napake** pomeni popravke hroščev in revizije, ki odpravljajo napake ali pomanjkljivosti, vključno z varnostnimi ranljivostmi, v elementih za dostavo.

**Ublažitev** pomeni kakršen koli način za zmanjšanje ali preprečenje tveganj za varnostno ranljivost.

**Varnostna ranljivost** pomeni stanje pri načrtovanju, kodiranju, razvijanju, uvajanju, preizkušanju, delovanju, podpiranju, vzdrževanju ali upravljanju elementa za dostavo, ki komur koli omogoča napad, ki lahko povzroči nepooblaščen dostopanje ali izkoriščanje, vključno z naslednjim: (a) dostopanje do, nadziranje ali prekinjanje delovanja sistema, (b) dostopanje do, brisanje, spreminjanje ali izvlečenje podatkov oziroma (c) spreminjanje identitete, pooblastil ali dovoljenj uporabnikov ali skrbnikov. Varnostna ranljivost lahko obstaja ne glede na to, ali ji je dodeljen ID CVE (splošne ranljivosti in izpostavljenosti) ali kakršna koli ocena ali uradna klasifikacija.

4.1 Dobavitelj izjavlja in jamči, da bo: (a) uporabljal najboljše panožne prakse za prepoznavanje varnostnih ranljivosti, vključno z neprekinjenim statičnim in dinamičnim pregledovanjem varnosti uporabe izvorne kode, pregledovanjem varnosti odprte kode in pregledovanjem ranljivosti sistema, (b) ravnal skladno z zahtevami teh določb, da bo pomagal preprečevati, zaznavati in odpravljati varnostne ranljivosti v elementih za dostavo in v vseh informacijskotehnoloških aplikacijah, platformah in infrastrukturi, v katerih in prek katerih dobavitelj ustvarja in zagotavlja storitve in elemente za dostavo.

4.2 Če bo dobavitelj izvedel za varnostno ranljivost v elementu za dostavo ali v kateri koli takšni informacijskotehnološki aplikaciji, platformi ali infrastrukturi, bo družbi Kyndryl zagotovil popravek napake in ublažitve za vse različice in izdaje elementov za dostavo v skladu z ravnmi resnosti in časovnimi okviri, opredeljenimi v spodnjih tabelah:

<b>Raven resnosti*</b>
<b>Urgentna varnostna ranljivost</b> – je varnostna ranljivost, ki predstavlja resno in potencialno globalno grožnjo. Kyndryl določa urgentne varnostne ranljivosti izključno po svoji presoji, ne glede na osnovno oceno CVSS.
<b>Kritična</b> – je varnostna ranljivost, ki ima osnovno oceno CVSS od 9 do 10,0
<b>Zelo resna</b> – je varnostna ranljivost, ki ima osnovno oceno CVSS od 7,0 do 8,9
<b>Srednje resna</b> – je varnostna ranljivost, ki ima osnovno oceno CVSS od 4,0 do 6,9
<b>Manj resna</b> – je varnostna ranljivost, ki ima osnovno oceno CVSS od 0,0 do 3,9

Časovni okviri				
<i>Urgentna</i>	<i>Kritična</i>	<i>Zelo resna</i>	<i>Srednje resna</i>	<i>Manj resna</i>
<i>4 dni ali manj, kot določijo v glavni pisarni za informacijsko varnost družbe Kyndryl</i>	30 dni	30 dni	90 dni	V skladu z najboljšimi panožnimi praksami

\* V vsakem primeru, kadar varnostna ranljivost nima že vnaprej dodeljene osnovne ocene CVSS, bo dobavitelj dodelil raven resnosti, ki je primerna za naravo in okoliščine takšne ranljivosti.

4.3 Dobavitelj bo za varnostno ranljivost, ki je bila javno razkrita in za katero dobavitelj družbi Kyndryl še ni zagotovil popravka napak ali ublažitve, uvedel vse tehnično izvedljive dodatne varnostne nadzore, ki lahko ublažijo tveganja ranljivosti.

4.4 Če Kyndryl ne bo zadovoljen z dobaviteljevim odzivom na kakršno koli varnostno ranljivost v elementu za dostavo ali kateri koli aplikaciji, platformi ali infrastrukturi, omenjeni zgoraj, bo dobavitelj brez poseganja v kakršne koli druge pravice družbe Kyndryl takoj uredil pogovor družbe Kyndryl neposredno z dobaviteljevim podpredsednikom ali enakovrednim izvršnim članom, ki je odgovoren za dostavo popravka napake.

4.5 Primeri varnostnih ranljivosti vključujejo kodo tretjih oseb ali odprto kodo s koncem storitve, kjer ti vrsti kode ne prejemata več varnostnih popravkov.

## ***Člen VI: Dostop do poslovnih sistemov***

Ta člen velja, če bodo imeli dobaviteljevi uslužbenci dostop do katerega koli poslovnega sistema.

### **1. Splošni pogoji**

1.1 Kyndryl bo določil, ali bo dobaviteljevim uslužbencem odobril dostop do poslovnih sistemov. Če Kyndryl dostop odobri, bo dobavitelj ravnal skladno z zahtevami tega člena in k takšnemu ravnanju zavezal tudi svoje uslužbenke s takšnim dostopom.

1.2 Kyndryl bo opredelil načine, na katere bodo lahko dobaviteljevi uslužbenci dostopali do poslovnih sistemov, vključno s tem, ali bodo ti uslužbenci dostopali do poslovnih sistemov prek naprav, ki jih bo zagotovil Kyndryl, ali naprav, ki jih bo zagotovil dobavitelj.

1.3 Dobaviteljevi uslužbenci lahko dostopajo do poslovnih sistemov in uporabljajo naprave, ki jih Kyndryl odobri za takšen dostop, samo za zagotavljanje storitev. Dobaviteljevi uslužbenci ne smejo uporabljati naprav, ki jih za to odobri Kyndryl, za zagotavljanje storitev kateri koli drugi osebi ali entiteti oziroma za dostopanje do informacijskotehnoloških sistemov, omrežij, aplikacij, spletnih mest, e-poštnih orodij, orodij za sodelovanje ali podobnih elementov dobavitelja ali tretje osebe v povezavi s storitvami.

1.4 V pojasnilo – dobaviteljevi uslužbenci ne smejo uporabljati naprav, ki jih Kyndryl odobri za dostop do poslovnih sistemov, za nobene osebne razloge (dobaviteljevi uslužbenci na primer v te naprave ne smejo shranjevati osebnih datotek, kot so glasba, videoposnetki, slike ali drugi podobni elementi, in v teh napravah ne smejo uporabljati interneta za osebne razloge).

1.5 Dobaviteljevi uslužbenci ne bodo kopirali materialov družbe Kyndryl, ki so dostopni prek poslovnega sistema, brez predhodne pisne odobritve družbe Kyndryl (in ne bodo nikoli kopirali katerih koli materialov družbe Kyndryl v prenosno napravo za shranjevanje, na primer na ključek USB, zunanji trdi disk ali drugo podobno napravo).

1.6 Dobavitelj bo na zahtevo poimensko po zaposlenih potrdil specifične poslovne sisteme, do katerih imajo njegovi zaposleni odobren dostop in do katerih so dostopali v kakršnem koli časovnem obdobju, ki ga določi Kyndryl.

1.7 Dobavitelj bo obvestil družbo Kyndryl v roku štiriindvajsetih (24) ur po tem, ko kateri koli dobaviteljev uslužbenec z dostopom do katerega koli poslovnega sistema ne bo več: (a) zaposlen pri dobavitelju ali (b) sodeloval pri dejavnostih, ki zahtevajo takšen dostop. Dobavitelj bo v sodelovanju z družbo Kyndryl zagotovil, da bo dostop za takšnega nekdanjega ali trenutnega uslužbenca nemudoma preklican.

1.8 Dobavitelj bo družbi Kyndryl nemudoma poročal o kakršnih koli dejanskih ali domnevnih varnostnih incidentih (kot so izguba naprave družbe Kyndryl ali dobavitelja oziroma nepooblaščen dostop do naprave ali podatkov, materialov ali drugih informacij kakršne koli vrste) in bo sodeloval z družbo Kyndryl pri preiskavi takšnih incidentov.

1.9 Dobavitelj brez predhodnega pisnega soglasja družbe Kyndryl ne sme nobenemu agentu, neodvisnemu pogodbeniku ali podizvajalčevemu uslužbencu dovoliti dostopa do katerega koli poslovnega sistema; če bo Kyndryl podal takšno soglasje, bo dobavitelj pogodbeno zavezal te osebe in njihove delodajalce k skladnosti z zahtevami tega člena, kot da bi bili dobaviteljevi uslužbenci, in bo družbi Kyndryl odgovarjal za vsa dejanja in opustitve dejanj katere koli takšne osebe ali delodajalca v zvezi s takšnim dostopom do poslovnega sistema.

### **2. Programska oprema naprav**

2.1 Dobavitelj bo naročil svojim uslužbencem, da morajo pravočasno namestiti vso programsko opremo naprave, ki jo zahteva Kyndryl za omogočanje varnega dostopa do poslovnih sistemov. Niti dobavitelj niti

njegovi uslužbenci ne bodo motili delovanja te programske opreme ali varnostnih funkcij, ki jih programska oprema omogoča.

2.2 Dobavitelj in njegovi uslužbenci bodo upoštevali konfiguracijska pravila naprave, ki jih nastavi Kyndryl, in tudi drugače v sodelovanju z družbo Kyndryl pomagali zagotoviti, da programska oprema deluje, kot želi Kyndryl. Dobavitelj na primer ne bo preglasil funkcij za blokiranje spletnih mest s programsko opremo ali samodejnega nameščanja popravkov.

2.3 Dobaviteljevi uslužbenci ne smejo naprav, s katerimi dostopajo do poslovnih sistemov, ali svojih uporabniških imen, gesel in podobnega za napravo, deliti z nobeno drugo osebo.

2.4 Če Kyndryl dobaviteljevemu uslužbencem odobri dostop do poslovnih sistemov z dobaviteljevimi napravami, bo dobavitelj v teh napravah namestil in izvajal operacijski sistem, ki ga odobri Kyndryl, in bo opravil nadgradnjo na novo različico tega operacijskega sistema ali na nov operacijski sistem v razumnem času po tem, ko mu Kyndryl to naroči.

### **3. Nadzor in sodelovanje**

3.1 Kyndryl ima brezpogojne pravice do nadziranja in saniranja potencialnih vdorov in drugih kibernetičnih varnostnih groženj na kakršen koli način, s katerih koli lokacij in z uporabo kakršnih koli ukrepov, za katere meni, da so potrebni ali primerni, in sicer brez predhodnega obvestila dobavitelju, kateremu koli dobaviteljevemu uslužbencu ali drugim. Kyndryl lahko na primer kadar koli (a) izvede preizkus varnosti v kateri koli napravi, (b) nadzira, pridobi na tehnološki ali drug način in pregleda komunikacije (vključno z e-poštnimi sporočili iz katerega koli e-poštnega računa), zapise, datoteke in druge elemente, shranjene v kateri koli napravi ali prenesene prek katerega koli poslovnega sistema, ter (c) pridobi celotno forenzično sliko katere koli naprave. Če Kyndryl za uveljavljanje svojih pravic potrebuje dobaviteljevo sodelovanje, bo dobavitelj v celoti in pravočasno izpolnil zahteve družbe Kyndryl za takšno sodelovanje (vključno z na primer zahtevami za varno konfiguriranje katere koli naprave, nameščanje nadzorne ali druge programske opreme v katero koli napravo, skupno rabo podrobnosti povezave na ravni sistema, vključevanje v ukrepe za odzivanje na incidente v kateri koli napravi ter zagotavljanje fizičnega dostopa do katere koli naprave, da lahko Kyndryl pridobi celotno forenzično sliko ali druge informacije, ter podobnimi in povezanimi zahtevami).

3.2 Če Kyndryl meni, da je to potrebno za njegovo zaščito, lahko kadar koli prekliče dostop do poslovnih sistemov kateremu koli dobaviteljevemu uslužbencu ali vsem dobaviteljevimi uslužbencem brez predhodnega obvestila dobavitelju ali kateremu koli dobaviteljevemu uslužbencu ali drugim.

3.3 Pravic družbe Kyndryl na noben način ne blokira, zmanjšuje ali omejuje nobena določba transakcijskega dokumenta, povezane osnovne pogodbe med pogodbenima strankama ali katere koli druge pogodbe med pogodbenima strankama, vključno s kakršno koli določbo, ki lahko zahteva, da se podatki, materiali ali druge informacije kakršne koli vrste nahajajo samo na izbrani lokaciji ali lokacijah, ali ki lahko zahteva, da samo osebe z izbrane lokacije ali lokacij dostopajo do takšnih podatkov, materialov ali drugih informacij.

### **4. Naprave družbe Kyndryl**

4.1 Kyndryl obdrži lastninsko pravico do vseh naprav družbe Kyndryl, dobavitelj pa prevzame tveganje za izgubo naprav, kar vključuje krajo, vandalizem ali malomarnost. Dobavitelj brez predhodnega pisnega soglasja družbe Kyndryl ne bo izvedel ali dovolil kakršnih koli sprememb naprav družbe Kyndryl, pri čemer sprememba pomeni kakršno koli spremembo naprave, vključno s spremembo programske opreme, aplikacij, varnostne zasnove oziroma fizične, mehanične ali električne zasnove naprave.

4.2 Dobavitelj bo vrnil vse naprave družbe Kyndryl v roku 5 delovnih dni po tem, ko preneha potreba po teh napravah za zagotavljanje storitev, in bo na zahtevo družbe Kyndryl sočasno uničil vse podatke, materiale in druge informacije kakršne koli vrste v teh napravah, ne da bi obdržal kakršno koli kopijo, z upoštevanjem najboljših panožnih praks za trajen izbris vseh takšnih podatkov, materialov in drugih informacij. Dobavitelj bo na svoje stroške zapakiral naprave družbe Kyndryl in jih vrnil na lokacijo, ki jo določi Kyndryl, v enakem stanju,

v kakršnem so bile dostavljene dobavitelju, z izjemo razumne obrabe. Če dobavitelj ne ravna skladno s katero koli obveznostjo v tem razdelku 4.2, to predstavlja hujšo kršitev transakcijskega dokumenta in povezane osnovne pogodbe in katere koli povezane pogodbe med pogodbenima strankama, pri čemer se razume, da je pogodba »povezana«, če dostop do katerega koli poslovnega sistema dobavitelju pomaga pri njegovih nalogah ali drugih aktivnostih v okviru te pogodbe.

4.3 Kyndryl bo zagotavljal podporo za naprave družbe Kyndryl (vključno s pregledovanjem naprav ter preventivnim in sanacijskim vzdrževanjem). Dobavitelj bo družbo Kyndryl takoj obvestil o potrebi po sanacijski storitvi.

4.4 Za programsko opremo, ki je v lasti družbe Kyndryl ali za katero ima ta pravico za licenciranje, Kyndryl dobavitelju podeljuje začasno pravico do uporabe, shranjevanja in izdelave zadostnega števila kopij, da podpre svojo pooblaščen uporabo naprav družbe Kyndryl. Dobavitelj ne sme prenesti programov nikomur, izdelovati kopij informacij o licenci za programsko opremo oziroma razstavljeni, povratno prevajati, izvajati povratnega inženirstva ali drugače prevajati katerega koli programa, razen če je to izrecno dovoljeno z veljavno zakonodajo in ni možnosti za pogodbeno odpoved pravici.

## **5. Posodobitve**

5.1 Ne glede na kakršne koli nasprotne določbe v transakcijskem dokumentu ali povezani osnovni pogodbi med pogodbenima strankama lahko Kyndryl s pisnim obvestilom in ne da bi potreboval dobaviteljevo soglasje, posodobi, dopolni ali drugače izboljša ta člen, da obravnava kakršno koli zahtevo v okviru veljavne zakonodaje ali obveznosti do naročnika, tako da odraža vse najboljše prakse glede razvoja in varnosti, ali drugače, kot Kyndryl meni, da je potrebno za zaščito poslovnih sistemov ali družbe Kyndryl.

## **Člen VII: Povečanje osebja**

Ta člen velja, če bodo dobaviteljevi uslužbenci posvetili ves svoj delovni čas zagotavljanju storitev za Kyndryl, izvajali vse te storitve na lokaciji družbe Kyndryl, na naročnikovi lokaciji ali od doma ter bodo storitve zagotavljali samo z uporabo naprav družbe Kyndryl za dostop do poslovnih sistemov.

### **1. Dostop do poslovnih sistemov; okolja družbe Kyndryl**

1.1 Dobavitelj lahko izvaja storitve samo tako, da dostopa do poslovnih sistemov z napravami, ki jih zagotovi Kyndryl.

1.2 Dobavitelj bo pri vsakem dostopu do poslovnih sistemov ravnal skladno z določbami, opredeljenimi v členu VI (Dostop do poslovnih sistemov).

1.3 Naprave, ki jih zagotovi Kyndryl, so edine naprave, ki jih lahko dobavitelj in njegovi uslužbenci uporabljajo za zagotavljanje storitev, dobavitelj in njegovi uslužbenci pa jih lahko uporabljajo samo za zagotavljanje storitev. V pojasnilo: dobavitelj ali njegovi uslužbenci za zagotavljanje storitev v nobenem primeru ne smejo uporabljati nobenih drugih naprav ali uporabljati naprav družbe Kyndryl za katerega koli drugega dobaviteljevega naročnika ali za kakršen koli drug namen, ki ni zagotavljanje storitev za Kyndryl.

1.4 Dobaviteljevi uslužbenci, ki uporabljajo naprave družbe Kyndryl, lahko delijo materiale družbe Kyndryl drug z drugim in jih shranjujejo v naprave družbe Kyndryl, vendar le v omejenem obsegu, v katerem je takšno deljenje in shranjevanje potrebno za uspešno izvajanje storitev.

1.5 Dobavitelj ali njegovi uslužbenci v nobenem primeru ne smejo odstraniti nobenih materialov družbe Kyndryl iz repozitorijev, okolij, orodij ali infrastrukture družbe Kyndryl, kjer jih hrani Kyndryl, razen v zvezi s takšnim shranjevanjem znotraj naprav družbe Kyndryl.

1.6 V pojasnilo: dobavitelj in njegovi uslužbenci brez predhodnega pisnega soglasja družbe Kyndryl nimajo pooblastila za prenos nobenih materialov družbe Kyndryl v nobene dobaviteljeve repozitorije, okolja, orodja ali infrastrukturo oziroma v nobene druge dobaviteljeve sisteme, platforme, omrežja ali podobno.

1.7 Člen VIII (Tehnični in organizacijski ukrepi, splošna varnost) ne veljajo za dobaviteljeve storitve, če bodo dobaviteljevi uslužbenci posvetili ves svoj delovni čas zagotavljanju storitev za Kyndryl, izvajali vse te storitve na lokaciji družbe Kyndryl, na naročnikovi lokaciji ali od doma ter bodo storitve zagotavljali samo z uporabo naprav družbe Kyndryl za dostop do poslovnih sistemov. V nasprotnem primeru za dobaviteljeve storitve velja člen VIII.



## **Člen VIII: Tehnični in organizacijski ukrepi, splošna varnost**

Ta člen velja, če dobavitelj družbi Kyndryl zagotavlja kakršne koli storitve ali elemente za dostavo, razen če bo imel dobavitelj pri zagotavljanju teh storitev in elementov za dostavo dostop samo do PKI družbe Kyndryl (tj. dobavitelj ne bo obdeloval nobenih drugih podatkov družbe Kyndryl ali imel dostopa do katerih koli drugih materialov družbe Kyndryl ali katerega koli poslovnega sistema), če je dobaviteljeva edina storitev in element za dostavo to, da družbi Kyndryl zagotavlja programsko opremo na mestu uporabe, oziroma če dobavitelj zagotavlja vse svoje storitve in elemente za dostavo po modelu povečanja osebja v skladu s členom VII, vključno z razdelkom 1.7 tega člena.

Dobavitelj bo ravnal skladno z zahtevami tega člena in s tem zaščitil: (a) materiale družbe Kyndryl pred izgubo, uničenjem, spreminjanjem, nenamernim ali nepooblaščenim razkritjem in nenamernim ali nepooblaščenim dostopom, (b) podatke družbe Kyndryl pred nezakonitimi oblikami obdelave ter (c) tehnologijo družbe Kyndryl pred nezakonitimi oblikami obravnavanja. Zahteve tega člena veljajo za vse informacijskotehnološke aplikacije, platforme in infrastrukturo, ki jih dobavitelj uporablja ali upravlja pri zagotavljanju elementov za dostavo in storitev ter pri obravnavanju tehnologije družbe Kyndryl, vključno z vsemi okolji za razvoj, preizkušanje, gostovanje, podporo, delovanje in podatkovne centre.

### **1. Varnostni pravilniki**

1.1 Dobavitelj bo vzdrževal in upošteval informacijskotehnološke varnostne pravilnike in prakse, ki so sestavni del dobaviteljevega poslovanja, obvezni za vse dobaviteljevo osebje in skladni z najboljšimi panožnimi praksami.

1.2 Dobavitelj bo vsaj enkrat letno pregledal svoje informacijskotehnološke varnostne pravilnike in prakse ter jih dopolnil tako, kot meni, da je potrebno za zaščito materialov družbe Kyndryl.

1.3 Dobavitelj bo vzdrževal in upošteval standardne in obvezne zahteve glede preverjanja zaposlitve za vse novozaposlene in razširil takšne zahteve na vse svoje osebje in hčerinske družbe, ki so v njegovi 100-odstotni lasti. Te zahteve bodo vključevale preverjanje nekaznovanosti v obsegu, ki ga dovoljujejo lokalni zakoni, preverjanje veljavnosti dokazila o identiteti in dodatna preverjanja, za katera dobavitelj meni, da so potrebna. Dobavitelj bo po potrebi redno ponavljal in ponovno preverjal te zahteve.

1.4 Dobavitelj bo svojim uslužbencem enkrat letno zagotovil izobraževanje glede varnosti in zasebnosti ter od vseh teh uslužbencev zahteval, da vsako leto potrdijo, da bodo ravnali skladno z dobaviteljevim kodeksom etičnega poslovanja, zaupnostjo in varnostnimi pravilniki, opredeljenimi v dobaviteljevem kodeksu ravnanja ali podobnih dokumentih. Dobavitelj bo osebam s skrbniškim dostopom do kakršnih koli sestavnih delov storitev, elementov za dostavo ali materialov družbe Kyndryl zagotovil dodatno usposabljanje glede pravilnikov in obdelave, pri čemer bo takšno usposabljanje značilno za njihovo vlogo in podporo pri storitvah, elementih za dostavo in materialih družbe Kyndryl ter kot je potrebno za vzdrževanje zahtevane skladnosti in certifikatov.

1.5 Dobavitelj bo načrtoval ukrepe glede varnosti in zasebnosti, s katerimi bo zaščitil in vzdrževal razpoložljivost materialov družbe Kyndryl, vključno s svojo uvedbo, vzdrževanjem in ravnanjem skladno s pravilniki in postopki, ki sami po sebi zahtevajo varnost in zasebnost, varno inženirstvo in varno delovanje, in sicer za vse storitve in elemente za dostavo ter za vso obravnavo tehnologije družbe Kyndryl.

### **2. Varnostni incidenti**

2.1 Dobavitelj bo vzdrževal in upošteval pravilnike o odzivanju na dokumentirane incidente, ki so skladni z najboljšimi panožnimi praksami za obravnavanje računalniških varnostnih incidentov.

2.2 Dobavitelj bo preiskal nepooblaščen dostop ali nepooblaščeno uporabo materialov družbe Kyndryl ter definirjal in izvršil ustrezen načrt odziva.

2.3 Dobavitelj bo nemudoma (najpozneje pa v 48 urah) obvestil družbo Kyndryl, ko bo izvedel za kakršno koli kršitev varnosti. Dobavitelj bo poslal takšno obvestilo na e-naslov: [cyber.incidents@kyndryl.com](mailto:cyber.incidents@kyndryl.com). Dobavitelj bo družbi Kyndryl zagotovil razumno zahtevane informacije o taki kršitvi in statusu morebitnih dobaviteljevih dejavnosti za sanacijo in obnovo. Razumno zahtevane informacije lahko na primer vključujejo dnevničke, ki prikazujejo privilegiran, skrbniški in drug dostop do naprav, sistemov ali aplikacij, forenzične slike naprav, sistemov ali aplikacij in druge podobne elemente, in sicer do mere, ki je primerna kršitvi ali dobaviteljevim dejavnostim za sanacijo in obnovitev.

2.4 Dobavitelj bo družbi Kyndryl zagotovil razumno pomoč pri izpolnjevanju kakršnih koli pravnih obveznosti (vključno z obveznostmi obveščanja regulatorjev ali oseb, na katere se nanašajo podatki) družbe Kyndryl, povezanih podjetij in naročnikov družbe Kyndryl (in njihovih naročnikov ali povezanih podjetij) v zvezi s kršitvijo varnosti.

2.5 Dobavitelj ne bo informiral ali obvestil nobene tretje osebe o tem, da je kršitev varnosti neposredno ali posredno povezana z družbo Kyndryl ali materiali družbe Kyndryl, razen če Kyndryl to pisno odobri ali to zahteva zakonodaja. Dobavitelj bo družbo Kyndryl pisno obvestil, preden bo distribuiral kakršno koli zakonsko zahtevano obvestilo kateri koli tretji osebi, če takšno obvestilo neposredno ali posredno razkriva identiteto družbe Kyndryl.

2.6 V primeru kršitve varnosti, ki izhaja iz dobaviteljeve kršitve katere koli obveznosti v okviru teh določb:

(a) bo dobavitelj odgovoren za vse stroške, ki jih utрпи sam, pa tudi za dejanske stroške, ki jih utрпи Kyndryl, pri zagotavljanju obvestila o kršitvi varnosti zadevnim regulatorjem, drugim vladnim ali ustreznim panožnim samoregulativnim agencijam, medijem (če to zahteva veljavna zakonodaja), osebam, na katere se nanašajo podatki, naročnikom in drugim;

(b) bo dobavitelj na zahtevo družbe Kyndryl na svoje stroške vzpostavil in vzdrževal klicni center za odgovarjanje na vprašanja oseb, na katere se nanašajo podatki, glede kršitve varnosti in njenih posledic, in sicer 1 leto po datumu, na katerega so bile takšne osebe, na katere se nanašajo podatki, obveščene o kršitvi varnosti, ali kot to zahteva kateri koli zakon o varstvu podatkov, kar koli od tega zagotavlja večjo zaščito. Kyndryl in dobavitelj bosta v sodelovanju ustvarila skripte in druge materiale, ki jih bo osebje klicnega centra uporabljalo pri odzivanju na poizvedbe. Kyndryl lahko na podlagi poslanega pisnega obvestila dobavitelju tudi sam vzpostavi in vzdržuje svoj klicni center, namesto da to naredi dobavitelj, dobavitelj pa bo družbi Kyndryl povrnil dejanske stroške, ki jih Kyndryl utрпи zaradi vzpostavitve in vzdrževanja takšnega klicnega centra; in

(c) bo dobavitelj družbi Kyndryl povrnil dejanske stroške, ki jih utрпи Kyndryl pri zagotavljanju storitev za spremljanje in obnavljanje kreditne sposobnosti v 1 letu po datumu, ko so bili posamezniki, na katere je vplivala kršitev in ki so se odločili registrirati za takšne storitve, obveščeni o kršitvi varnosti, ali kot to zahteva kateri koli zakon o varstvu podatkov, kar koli od tega zagotavlja večjo zaščito.

**3. Fizična varnost in nadzor vstopa** (izraz »objekt«, kot se uporablja v nadaljevanju, pomeni fizično lokacijo, na kateri dobavitelj gosti, obdeluje ali drugače dostopa do materialov družbe Kyndryl).

3.1 Dobavitelj bo vzdrževal ustrezne oblike nadzora fizičnega vstopa, kot so ovire, s karticami nadzorovane vstopne točke, nadzorne kamere in recepcije z osebjem, s katerimi bo preprečil nepooblaščen vstop v objekte.

3.2 Dobavitelj bo za dostop, vključno s kakršnim koli začasnim dostopom, do objektov in nadzorovanih območij znotraj objektov zahteval pooblaščenno odobritev, dostop pa bo omejil glede na vlogo na delovnem mestu in poslovno potrebo. Če bo dobavitelj odobril začasen dostop, bo njegov pooblaščen uslužbenec spremljal vsakega obiskovalca, ko bo ta v objektu in na katerih koli nadzorovanih območjih.

3.3 Dobavitelj bo uvedel oblike nadzora fizičnega dostopa, vključno z oblikami nadzora dostopa z več dejavniki, ki so skladne z najboljšimi panožnimi praksami, s katerimi bo ustrezno omejil vstop na nadzorovana območja znotraj objektov, in v dnevnik beležil vse poskuse vstopa, takšne dnevnike pa bo hranil vsaj eno leto.

3.4 Dobavitelj bo preklical dostop do objektov in nadzorovanih območij znotraj objektov (a) ob prenehanju delovnega razmerja s pooblaščenim dobaviteljevim uslužbencem ali (b) ko pooblaščen dobaviteljev uslužbenec ne bo več imel veljavne poslovne potrebe za dostop. Dobavitelj bo upošteval uradne postopke o dokumentiranem prenehanju delovnega razmerja, ki vključujejo takojšnjo odstranitev s seznamov za nadzor dostopa in predajo izkaznic za dostop.

3.5 Dobavitelj bo z varnostnimi ukrepi zaščitil vso fizično infrastrukturo, ki se uporablja za podpiranje storitev in elementov za dostavo ter obravnavanje tehnologije družbe Kyndryl, pred okoljskimi grožnjami, ki nastanejo naravno ali jih povzroči človek, kot so previsoka temperatura okolja, požar, poplava, vlažnost, kraja in vandalizem.

#### **4. Nadzor dostopa, posegov, prenosa in ločevanja**

4.1 Dobavitelj bo vzdrževal dokumentirano varnostno arhitekturo omrežij, ki jih uporablja pri svojem izvajanju storitev, zagotavljanju elementov za dostavo in obravnavanju tehnologije družbe Kyndryl. Dobavitelj bo ločeno pregledoval takšno arhitekturo omrežij in vpeljal ukrepe za preprečevanje nepooblaščenih omrežnih povezav do sistemov, aplikacij in omrežnih naprav za zagotavljanje skladnosti s poglobljenimi standardi glede varne segmentacije, izolacije in obrambe. Dobavitelj pri gostovanju ali izvajanju katerih koli gostovanih storitev ne sme uporabljati brezžične tehnologije, lahko pa jo uporablja pri zagotavljanju storitev in elementov za dostavo ter pri obravnavanju tehnologije družbe Kyndryl, vendar mora dobavitelj šifrirati in zahtevati varno preverjanje pristnosti za vsa takšna brezžična omrežja.

4.2 Dobavitelj bo izvajal ukrepe, zasnovane za logično ločevanje materialov družbe Kyndryl in preprečevanje, da bi bili izpostavljeni nepooblaščenim osebam ali da bi te osebe dostopale do njih. Dobavitelj bo tudi vzdrževal ustrezno izolacijo svojih produkcijskih, neprodukcijskih in drugih okolij, hkrati pa bo – če so materiali družbe Kyndryl že prisotni v neprodukcijskem okolju ali preneseni vanj (na primer za reproduciranje napake) – dobavitelj zagotovil, da je zaščita glede varnosti in zasebnosti v neprodukcijskem okolju enaka tisti v produkcijskem okolju.

4.3 Dobavitelj bo šifriral materiale družbe Kyndryl v tranzitu in v mirovanju (razen če dobavitelj družbi Kyndryl razumno in zadovoljivo prikaže, da je šifriranje materialov družbe Kyndryl v mirovanju tehnično neizvedljivo). Dobavitelj bo šifriral tudi vse fizične medije, če obstajajo, na primer medije, ki vsebujejo datoteke varnostnih kopij. Dobavitelj bo dokumentiral postopke za generiranje, izdajo, distribucijo, shranjevanje, izmenjevanje, preklic, obnovitev, varnostno kopiranje, uničenje, dostop in uporabo varnostnih ključev, povezanih s šifriranjem podatkov. Dobavitelj bo zagotovil, da bodo specifične kriptografske metode, uporabljene za takšno šifriranje, v skladu z najboljšimi panožnimi praksami (kot je NIST SP 800-131a).

4.4 Če dobavitelj potrebuje dostop do materialov družbe Kyndryl, bo tak dostop omejil na najnižjo raven, potrebno za zagotavljanje in podpiranje storitev in elementov za dostavo. Dobavitelj bo zahteval, da bo takšen dostop, vključno s skrbniškim dostopom do kakršnih koli temeljnih komponent (tj. privilegiran dostop), individualen, da bo temeljil na vlogah in da bo predmet odobritve in rednega preverjanja veljavnosti s strani pooblaščenih dobaviteljevih uslužbencev, ki bodo upoštevali načela ločitve dolžnosti. Dobavitelj bo vzdrževal ukrepe za identificiranje in odstranjevanje odvečnih in mirujočih računov. Dobavitelj bo prav tako preklical račune s privilegiranim dostopom v roku štiriindvajsetih (24) ur po prenehanju delovnega razmerja z lastnikom računa ali na zahtevo družbe Kyndryl ali katerega koli pooblaščenega dobaviteljevega uslužbenca, npr. vodje lastnika računa.

4.5 Dobavitelj bo v skladu z najboljšimi panožnimi praksami vzdrževal tehnične ukrepe, ki bodo uveljavljali časovno omejitev neaktivnih sej, zaklepanje računov po večkratnih zaporednih neuspešnih poskusih prijave in preverjanje pristnosti z močnim geslom, ter ukrepe, ki bodo zahtevali varen prenos in shranjevanje takšnih gesel. Poleg tega bo dobavitelj uporabljal večkratno preverjanje pristnosti za vsak privilegiran dostop do katerih koli materialov družbe Kyndryl, ki ne temelji na konzoli.

4.6 Dobavitelj bo nadzoroval uporabo privilegiranega dostopa in vzdrževal varnostne informacije in ukrepe za upravljanje dogodkov, načrtovane za: (a) identificiranje nepooblaščenega dostopa in dejavnosti, (b) omogočanje pravočasnega in ustreznega odziva na takšen dostop in dejavnost ter (c) omogočanje revizij s strani dobavitelja, družbe Kyndryl (v skladu z njenimi pravicami do preverjanja v teh določbah in pravic do beleženja v transakcijskem dokumentu ali povezani osnovni ali drugi povezani pogodbi med pogodbenima strankama) in drugih v skladu z dokumentiranim pravilnikom dobavitelja.

4.7 Dobavitelj bo hranil dnevnike, v katerih bo v skladu z najboljšimi panožnimi praksami beležil vse skrbniške, uporabniške in druge dostope ali dejavnosti v zvezi s sistemi, ki se uporabljajo pri zagotavljanju storitev ali elementov za dostavo in obravnavanju tehnologije družbe Kyndryl (in bo te dnevnike na zahtevo zagotovil družbi Kyndryl). Dobavitelj bo vzdrževal ukrepe, načrtovane za zaščito pred nepooblaščenim dostopom, spreminjanjem in nenamernim ali namernim uničenjem takšnih dnevnikov.

4.8 Dobavitelj bo vzdrževal računalniške zaščite za sisteme, ki jih ima v lasti ali jih upravlja, vključno s sistemi končnih uporabnikov, in ki jih uporablja pri zagotavljanju storitev ali elementov za dostavo oziroma pri obravnavanju tehnologije družbe Kyndryl, pri čemer bodo takšne zaščite vključevale: požarne zidove končnih točk, šifriranje celotnega diska, zaznavanje končne točke s podpisom in brez podpisa ter tehnologije odzivanja

za obravnavanje zlonamerne programske opreme in naprednih vztrajnih groženj, zaklepanje zaslona na osnovi časa ter rešitve za upravljanje končnih točk, ki uveljavljajo zahteve glede konfiguracije zaščite in nameščanja popravkov. Poleg tega bo dobavitelj uvedel tehnične in operativne nadzore, ki bodo zagotavljali, da lahko dobaviteljeva omrežja uporabljajo samo znani in zaupanja vredni sistemi končnih uporabnikov.

4.9 Dobavitelj bo v skladu z najboljšimi panožnimi praksami vzdrževal zaščite za okolja podatkovnih centrov, v katerih so prisotni ali obdelani materiali družbe Kyndryl, pri čemer bodo takšne zaščite vključevale zaznavanje in preprečevanje vdorov ter protiukrepe in ublažitev za napade na omrežje, ki povzročijo odpoved njegovega delovanja.

## **5. Nadzor integritete storitev in sistemov ter razpoložljivosti**

5.1 Dobavitelj bo: (a) vsaj enkrat letno opravil oceno tveganja glede varnosti in zasebnosti, (b) izvedel preizkušanje varnosti in ocenil ranljivosti, vključno z avtomatiziranim pregledom varnosti sistemov in aplikacij ter ročnim etičnim hekanjem, in sicer pred produkcijsko izdajo in nato enkrat letno v zvezi s storitvami in elementi za dostavo ter enkrat letno v zvezi s svojim obravnavanjem tehnologije družbe Kyndryl, (c) najel usposobljeno neodvisno tretjo osebo, ki bo vsaj enkrat letno izvedla penetracijsko preizkušanje v skladu z najboljšimi panožnimi praksami, pri čemer bo takšno preizkušanje vključevalo tako avtomatizirano kot tudi ročno preizkušanje, (d) izvedel avtomatizirano upravljanje in rutinsko preverjanje skladnosti z zahtevami konfiguracije zaščite za vsak sestavni del storitev in elementov za dostavo in v zvezi s svojim obravnavanjem tehnologije družbe Kyndryl, ter (e) saniral identificirane ranljivosti ali neskladnosti z zahtevami konfiguracije zaščite na osnovi povezanega tveganja, možnosti zlorabe in vpliva. Dobavitelj bo izvedel razumne ukrepe, s katerimi se bo izognil prekinitvi delovanja storitev med izvajanjem preizkusov, ocen, pregledov in sanacijskih dejavnosti. Dobavitelj bo družbi Kyndryl na njeno zahtevo zagotovil pisni povzetek dobaviteljevih takrat najnovejših dejavnosti penetracijskega preizkušanja, poročilo pa bo vključevalo najmanj imena ponudb, ki jih je obsegalo preizkušanje, število sistemov ali aplikacij v obsegu preizkušanja, datume preizkušanja, metodologijo, uporabljeno pri preizkušanju, ter splošni povzetek ugotovitev.

5.2 Dobavitelj bo vzdrževal pravilnike in postopke, načrtovane za upravljanje tveganj, povezanih z uvajanjem sprememb v storitve ali elemente za dostavo oziroma obravnavanje tehnologije družbe Kyndryl. Dobavitelj bo pred uvedbo takšne spremembe, vključno s spremembo sistemov, omrežij in temeljnih sestavnih delov, na katere takšna sprememba vpliva, v registrirani zahtevi za spremembo dokumentiral naslednje: (a) opis spremembe in razlog zanjo, (b) podrobnosti in časovni razpored uvedbe, (c) izjavo o tveganju, ki obravnava vpliv na storitve in elemente za dostavo, naročnike storitev ali materiale družbe Kyndryl, (d) pričakovani rezultat, (e) načrt za razveljavitev in (f) odobritev pooblaščenih dobaviteljevih uslužbencev.

5.3 Dobavitelj bo vzdrževal seznam vseh informacijskotehnoških sredstev, ki jih uporablja pri delovanju storitev, zagotavljanju elementov za dostavo in obravnavanju tehnologije družbe Kyndryl. Dobavitelj bo redno nadziral in upravljal stanje (vključno z zmogljivostjo) in razpoložljivost takšnih informacijskotehnoških sredstev, storitev, elementov za dostavo in tehnologije družbe Kyndryl, vključno s temeljnimi sestavnimi deli takšnih sredstev, storitev, elementov za dostavo in tehnologije družbe Kyndryl.

5.4 Dobavitelj bo vse sisteme, ki jih bo uporabljal pri razvoju ali delovanju storitev in elementov za dostavo ter pri obravnavanju tehnologije družbe Kyndryl, zgradil iz preddefiniranih slik systemske varnosti ali varnostnih osnovnic, ki ustrezajo najboljšim panožnim praksam, kot so primerjalni preskusi CIS (Center for Internet Security).

5.5 Dobavitelj bo brez omejevanja svojih obveznosti ali pravic družbe Kyndryl v okviru transakcijskega dokumenta ali povezane osnovne pogodbe med pogodbenima strankama v zvezi s poslovno kontinuiteto ločeno ocenil vsako storitev in element za dostavo in vsak informacijskotehnoški sistem, ki se uporablja pri obravnavanju tehnologije družbe Kyndryl, glede poslovne in informacijskotehnoške kontinuitete in zahtev za obnovitev po katastrofi v skladu z dokumentiranimi smernicami za upravljanje tveganj. Dobavitelj bo zagotovil, da bo imela vsaka takšna storitev, element za dostavo in informacijskotehnoški sistem v obsegu, ki ga jamči takšna ocena tveganja, ločeno definirane, dokumentirane, vzdrževane in letno preverjene načrte za poslovno in informacijskotehnoško kontinuiteto ter obnovitev po katastrofi, ki bodo skladni z najboljšimi panožnimi praksami. Dobavitelj bo zagotovil, da so takšni načrti zasnovani za zagotavljanje specifičnih časov obnovitve, ki so opredeljeni v spodnjem razdelku 5.6.

5.6 Specifični cilji glede točke obnovitve (»**RPO**«) in cilji glede časa obnovitve (»**RTO**«) v zvezi s katero koli gostovano storitvijo so: 24 ur za RPO in 24 ur za RTO; kljub temu bo dobavitelj ravnal skladno z vsakim krajšim trajanjem RPO ali RTO, za katerega se bo Kyndryl zavezal naročniku, in sicer takoj po tem, ko bo Kyndryl pisno obvestil dobavitelja o takšnem krajšem trajanju RPO ali RTO (e-pošta šteje za pisno obvestilo). V zvezi z vsemi drugimi storitvami, ki jih dobavitelj zagotavlja družbi Kyndryl, bo dobavitelj zagotovil, da bodo njegovi načrti za poslovno kontinuiteto in obnovitev po katastrofi zasnovani za zagotavljanje RPO in RTO, ki dobavitelju omogočata ohranjanje skladnosti z vsemi njegovimi obveznostmi do družbe Kyndryl v okviru transakcijskega dokumenta in povezane osnovne pogodbe med pogodbenima strankama ter teh določb, vključno z njegovimi obveznostmi glede pravočasnega preizkušanja, podpiranja in vzdrževanja.

5.7 Dobavitelj bo vzdrževal ukrepe, zasnovane za ocenjevanje, preizkušanje in uveljavljanje varnostnih svetovalnih popravkov v storitvah in elementih za dostavo ter povezanih sistemih, omrežjih, aplikacijah in temeljnih sestavnih delih v obsegu teh storitev in elementov za dostavo, pa tudi v sistemih, omrežjih, aplikacijah in temeljnih sestavnih delih, ki se uporabljajo za obravnavanje tehnologije družbe Kyndryl. Po ugotovitvi, da je varnostni svetovalni popravek veljaven in ustrezen, ga bo dobavitelj uvedel v skladu z dokumentirano resnostjo in smernicami za oceno tveganja. Dobaviteljeva uvedba varnostnih svetovalnih popravkov bo izvedena skladno z njegovim pravilnikom o upravljanju sprememb.

5.8 Če ima Kyndryl razumno podlago za mnenje, da lahko strojna ali programska oprema, ki jo dobavitelj zagotavlja družbi Kyndryl, vsebuje elemente za vdiranje, kot so vohunska programska oprema, zlonamerna programska oprema ali zlonamerna koda, bo dobavitelj pravočasno v sodelovanju z družbo Kyndryl preiskal in odpravil njene pomisleke.

## **6. Zagotavljanje storitev**

6.1 Dobavitelj bo podpiral v panogi običajne metode za federativno preverjanje pristnosti za vse uporabniške ali naročniške račune družbe Kyndryl, pri čemer bo dobavitelj upošteval najboljše panožne prakse za preverjanje pristnosti takšnih uporabniških ali naročniških računov družbe Kyndryl (kot je centralno upravljana večstopenjska enotna prijava Kyndryl, ki uporablja OpenID Connect ali jezik SAML (Security Assertion Markup Language)).

**7. Podizvajalci.** Dobavitelj bo brez omejevanja svojih obveznosti ali pravic družbe Kyndryl v okviru transakcijskega dokumenta ali povezane osnovne pogodbe med pogodbenima strankama v zvezi z obdržanjem podizvajalcev zagotovil, da bo vsak podizvajalec, ki bo opravljal delo za dobavitelja, uvedel nadzore upravljanja za skladnost z zahtevami in obveznostmi, ki jih te določbe nalagajo dobavitelju.

**8. Fizični mediji.** Dobavitelj bo v skladu z najboljšimi panožnimi praksami za čiščenje medijev pred ponovno uporabo varno očistil fizične medije, ki so namenjeni ponovni uporabi, in uničil fizične medije, ki niso namenjeni ponovni uporabi.

### Člen IX: *Certifikati in poročila gostovanih storitev*

Ta člen velja, če dobavitelj družbi Kyndryl zagotavlja gostovano storitev.

1.1 Dobavitelj bo pridobil naslednje certifikate ali poročila v časovnih okvirjih, opredeljenih spodaj:

Certifikati/poročila	Časovni okvir
<p><b>V zvezi z dobaviteljevimi gostovanimi storitvami:</b></p> <p>certifikat o skladnosti s standardom ISO 27001, Informacijska tehnologija – Varnostne tehnike – Sistemi upravljanja informacijske varnosti, pri čemer bo to certifikat na osnovi ocene uglednega neodvisnega revizorja</p> <p><b>ali</b></p> <p>SOC 2 tipa 2: poročilo uglednega neodvisnega revizorja, ki izkazuje njegov pregled dobaviteljevih sistemov, nadzorov in delovanja v skladu s poročilom SOC 2 tipa 2 (ki vključuje vsaj varnost, zaupnost in razpoložljivost)</p>	<p>Dobavitelj bo pridobil certifikat o skladnosti s standardom ISO 27001 v 120 dneh po datumu veljavnosti transakcijskega dokumenta* ali datumu prevzema**, nato pa bo vsakih 12 mesecev po tem podaljševal veljavnost certifikata na osnovi ocene uglednega neodvisnega revizorja (vsako podaljšanje pa bo v skladu s takrat najnovejšo različico standarda)</p> <p>Dobavitelj bo pridobil poročilo SOC 2 tipa 2 v 240 dneh po datumu veljavnosti transakcijskega dokumenta* ali datumu prevzema**, nato pa bo vsakih 12 mesecev po tem pridobil novo poročilo uglednega neodvisnega revizorja, ki bo izkazovalo njegov pregled dobaviteljevih sistemov, nadzorov in delovanja v skladu s poročilom SOC 2 tipa 2 (ki vključuje vsaj varnost, zaupnost in razpoložljivost).</p> <p>* Če dobavitelj zagotavlja gostovano storitev od takšnega datuma veljavnosti.</p> <p>** Datum, s katerim dobavitelj prevzame obveznost zagotavljanja gostovane storitve.</p>

1.2 Če dobavitelj to pisno zahteva in Kyndryl to pisno odobri, lahko dobavitelj pridobi certifikat ali poročilo, ki je v bistvenih značilnostih enakovreden/-dno tistim, navedenim zgoraj, pri čemer se razume, da časovni okvirji, opredeljeni v zgornji tabeli, veljajo v nespremenjeni obliki za tak enakovreden certifikat ali poročilo.

1.3 Dobavitelj bo: (a) na zahtevo družbi Kyndryl takoj zagotovil kopijo vsakega certifikata in poročila, ki ga mora pridobiti dobavitelj, in (b) nemudoma odpravil kakršne koli notranje nadzorne pomanjkljivosti, opažene med pregledom SOC 2 ali v bistvenih značilnostih enakovrednim pregledom (če ga odobri Kyndryl).

## **Člen X: Sodelovanje, preverjanje in sanacija**

Ta člen velja, če dobavitelj družbi Kyndryl zagotavlja kakršno koli storitev ali element za dostavo.

### **1. Sodelovanje z dobaviteljem**

1.1 Če se Kyndryl upravičeno sprašuje, ali so katere koli storitve ali elementi za dostavo morda prispevali, prispevajo ali bodo prispevali h kakršnemu koli pomisleku glede kibernetne varnosti, bo dobavitelj razumno sodeloval pri kakršnem koli poizvedovanju družbe Kyndryl o takšnem pomisleku, vključno s pravočasnim in celovitim odzivanjem na zahteve za informacije, bodisi v obliki dokumentov, drugih zapisov, pogovorov z ustreznim dobaviteljevim osebjem ali podobnega.

1.2 Pogodbeni stranki se strinjata, da: (a) bosta na zahtevo oskrbeli druga drugo s takšnimi nadaljnjimi informacijami, (b) bosta potrdili in dostavili druga drugi takšne druge dokumente in (c) opravili takšna druga dejanja ali opravila, ki jih druga pogodbeni stranka lahko razumno zahteva za namen izvršitve namena teh določb in dokumentov, na katere se te določbe sklicujejo. Če na primer Kyndryl to zahteva, bo dobavitelj pravočasno zagotovil določbe glede zasebnosti in varnosti iz svojih pisnih pogodb s podobdelovalci in podizvajalci, vključno z odobritvijo dostopa do samih pogodb, če ima dobavitelj do tega pravico.

1.3 Če bo Kyndryl to zahteval, bo dobavitelj pravočasno zagotovil informacije o državah, v katerih so bili elementi za dostavo in sestavni deli teh elementov za dostavo proizvedeni, razviti ali drugače pridobljeni.

**2. Preverjanje** (izraz »objekt«, kot se uporablja v nadaljevanju, pomeni fizično lokacijo, na kateri dobavitelj gosti, obdeluje ali drugače dostopa do materialov družbe Kyndryl)

2.1 Dobavitelj bo vzdrževal evidenco, ki omogoča revizijo in izkazuje skladnost s temi določbami.

2.2 Kyndryl lahko sam ali z zunanjim revizorjem v skladu s pisnim obvestilom, ki ga 30 dni prej pošlje dobavitelju, preveri dobaviteljevo skladnost s temi določbami, vključno z dostopom do katerega koli objekta ali objektov za takšne namene, vendar Kyndryl ne bo dostopal do nobenega podatkovnega centra, v katerem dobavitelj obdeluje podatke družbe Kyndryl, razen če v dobri veri verjame, da bi to zagotovilo potrebne informacije. Dobavitelj bo sodeloval pri preverjanju družbe Kyndryl, vključno s pravočasnim in celovitim odzivanjem na zahteve za informacije v obliki dokumentov, drugih zapisov, pogovorov z ustreznim dobaviteljevim osebjem in podobnega. Dobavitelj lahko družbi Kyndryl v obravnavo ponudi dokazilo o upoštevanju odobrenega kodeksa ravnanja ali panožnega certifikata oziroma drugače zagotovi informacije, ki izkazujejo skladnost s temi določbami.

2.3 Preverjanje se ne bo izvajalo pogosteje kot enkrat v katerem koli 12-mesečnem obdobju, razen če: (a) Kyndryl preverja dobaviteljevo odpravo pomislekov, do katerih je prišlo med prejšnjim preverjanjem v 12-mesečnem obdobju, ali (b) je prišlo do kršitve varnosti in želi Kyndryl preveriti skladnost z obveznostmi, ki zadevajo kršitev. V obeh primerih bo Kyndryl 30 dni pred tem zagotovil enako pisno obvestilo, kot je opredeljeno v zgornjem razdelku 2.2, vendar lahko nujnost obravnavanja kršitve varnosti zahteva, da Kyndryl opravi preverjanje prej kot v 30 dneh po pošiljanju pisnega obvestila.

2.4 Regulator ali drug upravljavec lahko uveljavlja enake pravice kot Kyndryl iz razdelkov 2.2 in 2.3, pri čemer se razume, da lahko regulator uveljavlja kakršne koli dodatne pravice, ki jih ima v okviru zakonodaje.

2.5 Če ima Kyndryl razumno podlago za sklepanje, da dobavitelj ne ravna skladno s katero koli od teh določb (ne glede na to, ali takšna podlaga izvira iz preverjanja v okviru teh določb ali od drugod), bo dobavitelj takoj odpravil takšno neskladnost.

### **3. Program za preprečevanje ponarejanja**

3.1 Če dobaviteljevi elementi za dostavo vključujejo elektronske sestavne dele (npr. trde diske, polprevodniške pogone, pomnilnik, centralne procesne enote, logične naprave ali kable), bo dobavitelj vzdrževal in upošteval program za preprečevanje ponarejanja, ki bo predvsem preprečeval dobavitelju, da bi družbi Kyndryl zagotovil ponarejene sestavne dele, dodatno pa takoj zaznal in saniral vsak primer, v katerem bi dobavitelj družbi Kyndryl pomotoma zagotovil ponarejene sestavne dele. Dobavitelj bo k tej isti obveznosti za vzdrževanje in upoštevanje dokumentiranega programa za preprečevanje ponarejanja zavezal vse svoje dobavitelje, ki zagotavljajo elektronske sestavne dele, vključene v dobaviteljeve elemente za dostavo za Kyndryl.

### **4. Sanacija**

4.1 Če dobavitelj ne bo ravnal skladno s katero koli svojo obveznostjo v okviru teh določb in bo to neskladno ravnanje povzročilo kršitev varnosti, bo dobavitelj popravil neskladno ravnanje pri svojem izvajanju ter saniral škodljive učinke kršitve varnosti, pri čemer bo takšno izvajanje in saniranje potekalo v skladu z razumnimi navodili in urnikom družbe Kyndryl. Če pa kršitev varnosti izhaja iz dobaviteljeve preskrbe večnajemniške gostovane storitve in posledično vpliva na veliko dobaviteljevih strank, vključno z družbo Kyndryl, bo dobavitelj glede na naravo kršitve varnosti pravočasno in ustrezno popravil napako pri svojem izvajanju ter saniral škodljive učinke kršitve varnosti, pri tem pa ustrezno upošteval kakršne koli informacije družbe Kyndryl glede takšnih popravkov in sanacije. Brez poseganja v zgoraj navedeno mora dobavitelj brez nepotrebnega odlašanja obvestiti družbo Kyndryl, če ne more več izpolnjevati obveznosti, ki jih določa veljavna zakonodaja o varstvu podatkov.

4.2 Kyndryl ima pravico sodelovati pri sanaciji katere koli kršitve varnosti, navedene v razdelku 4.1, kot meni, da je ustrezno ali potrebno, dobavitelj pa bo odgovoren za vse stroške in izdatke popravila svojega izvajanja ter za stroške in izdatke sanacije, ki jih utrpita pogodbeni stranki v povezavi s katero koli takšno kršitvijo varnosti.

4.3 Stroški in izdatki sanacije, povezani s kršitvijo varnosti, lahko na primer vključujejo stroške zaznavanja in preiskovanja kršitve varnosti, določanja odgovornosti v okviru veljavnih zakonov in predpisov, zagotavljanja obvestil o kršitvi, vzpostavljanja in vzdrževanja klicnih centrov, zagotavljanja storitev za spremljanje in obnavljanje kreditne sposobnosti, ponovnega nalaganja podatkov, popravljanja okvar izdelkov (vključno prek izvorne kode ali drugega razvoja), najemanja tretjih oseb za pomoč pri prej omenjenih in drugih ustreznih dejavnostih ter druge stroške, ki so potrebni za sanacijo škodljivih učinkov kršitve varnosti. V pojasnilo: stroški sanacije ne vključujejo izgube dobička, poslovanja, vrednosti, prihodkov dobrega imena ali pričakovanih prihrankov družbe Kyndryl.