Articolo I, Informazioni di Contatto Commerciali

Questo Articolo si applica se il Fornitore o Kyndryl Tratta le BCI dell'altra parte.

1.1 Kyndryl e il Fornitore possono Trattare le BCI dell'altra parte ovunque queste si trovino a fare business in relazione alla esecuzione o consegna di Servizi o Materiali da Consegnare da parte del Fornitore.

1.2 Una parte:

a) non utilizzerà o divulgherà le BCI dell'altra parte per nessun altro scopo (per chiarezza, nessuna delle parti Venderà le BCI dell'altra parte o utilizzerà o divulgherà le BCI dell'altra parte per qualsiasi scopo di marketing senza previo consenso scritto dell'altra parte e, ove richiesto, il precedente consenso scritto degli Interessati) e

b) eliminerà, modificherà, correggerà, restituirà, fornirà informazioni sul Trattamento, limiterà il Trattamento o intraprenderà qualsiasi altra azione ragionevolmente richiesta nei confronti delle BCI dell'altra parte, tempestivamente su richiesta scritta dell'altra parte.

1.3 Le parti non stabiliscono un rapporto di cotitolarità come Titolare del Trattamento dei Dati Personali in relazione alle BCI dell'altra parte e nessuna disposizione del Documento d'Ordine sarà interpretata come indicante l'intenzione di stabilire un rapporto congiunto da Titolare del Trattamento dei Dati Personali.

1.4 La Dichiarazione Kyndryl sulla Privacy (Kyndryl Privacy Statement) disponibile alla pagina web https://www.kyndryl.com/privacy contiene ulteriori dettagli sul Trattamento da parte di Kyndryl delle BCI.

1.5 Le parti hanno implementato e manterranno misure di sicurezza tecniche e organizzative per proteggere le BCI di altri soggetti da perdita, distruzione, alterazione, divulgazione accidentale o non autorizzata, accesso accidentale o non autorizzato ed Trattamento illecito.

1.6 Il Fornitore informerà tempestivamente (e in ogni caso entro e non oltre 48 ore) Kyndryl dopo essere venuto a conoscenza di qualsiasi Violazione della Sicurezza che coinvolga il BCI di Kyndryl. Il fornitore fornirà tale notifica a cyber.incidents@kyndryl.com. Il Fornitore consegnerà a Kyndryl le informazioni ragionevolmente richieste su tale violazione e sullo stato di qualsiasi attività di correzione e rimedio intrapresa dal Fornitore. A titolo di esempio, le informazioni ragionevolmente richieste possono includere log che dimostrino l'avvenuto accesso privilegiato, amministrativo e di altro tipo a Dispositivi, sistemi o applicazioni, immagini forensi di Dispositivi, sistemi o applicazioni e altri elementi simili, nella misura in cui ciò sia pertinente alla violazione o alle attività di ripristino e rimedio poste in essere dal Fornitore.

1.7 Laddove il fornitore stia solo Trattando le BCI di Kyndryl e non abbia accesso ad altri dati o materiali di alcun tipo o a alcun Sistema Aziendale Kyndryl, questo articolo e l'articolo X (Cooperazione, Verifica e Rimedio) saranno gli unici articoli applicabili a tale Trattamento.

Articolo II, Misure Tecniche e Organizzative (TOMs), Sicurezza dei Dati

Questo Articolo si applica se il Fornitore Tratta Dati Kyndryl, diversi dalle BCI di Kyndryl. Il Fornitore si atterrà ai requisiti del presente Articolo fornendo tutti i Servizi e i Materiali da Consegnare e, in tal modo, proteggerà i Dati Kyndryl da perdita, distruzione, alterazione, divulgazione accidentale o non autorizzata, accesso accidentale o non autorizzato e forme illegali di Trattamento. I requisiti di questo Articolo si estendono a tutte le applicazioni, piattaforme e infrastrutture IT su cui il fornitore opera o che gestisce durante la fornitura dei Materiali da Consegnare e dei Servizi, inclusi tutti gli ambienti operativi di sviluppo, test, hosting, supporto ed i data center.

1. Uso dei Dati

1.1. Il Fornitore non può aggiungere ai Dati Kyndryl o includere con i Dati Kyndryl, senza il previo consenso scritto di Kyndryl, qualsiasi altra informazione o dato, inclusi eventuali Dati Personali, ed il Fornitore non può utilizzare i Dati Kyndryl in qualsiasi forma, aggregata o diversa, per qualsiasi scopo diverso dall'erogazione dei Servizi e dei Materiali da Consegnare (a titolo esemplificativo, al Fornitore non è consentito utilizzare o riutilizzare Dati Kyndryl per valutare l'efficacia o per sviluppare metodi per il miglioramento delle offerte del Fornitore, per ricerca e sviluppo atti a creare nuove offerte o a generare report relativi alle offerte del Fornitore). Se non espressamente consentito nel Documento d'Ordine, al Fornitore è vietato Vendere Dati Kyndryl.

1.2. Il Fornitore non incorporerà alcuna tecnologia di tracciamento Web nei Materiali da Consegnare o come parte dei Servizi (tali tecnologie includono HTML5, archiviazione locale, tag o token di terze parti e Web beacon) se non espressamente consentito nel Documento d'Ordine.

2. Richieste di Terzi e Riservatezza

2.1. Il Fornitore non divulgherà i Dati Kyndryl a qualsiasi terza parte, salvo non venga autorizzato anticipatamente da Kyndryl per iscritto. Se un governo, incluso qualsiasi organismo regolatore, dovesse richiedere l'accesso ai Dati Kyndryl (ad es. se il governo degli Stati Uniti richiedesse al Fornitore di fornire i Dati Kyndryl per motivi di sicurezza nazionale), o se una divulgazione dei Dati Kyndryl venisse altrimenti richiesta dalla legge, il Fornitore informerà Kyndryl per iscritto di tale richiesta o requisito e offrirebbe a Kyndryl una ragionevole opportunità di contestare qualsiasi divulgazione (laddove la legge vieti la notifica, il Fornitore intraprenderà le misure che ritiene ragionevolmente appropriate per contestare il divieto e la divulgazione dei Dati Kyndryl attraverso azioni giudiziarie o altri mezzi).

2.2. Il Fornitore assicura a Kyndryl che: (a) tale accesso sarà concesso solo ai propri dipendenti che hanno avranno bisogno di accedere a Dati Kyndryl per erogare Servizi o i Materiali da Consegnare, e solo nella misura necessaria per fornire tali Servizi e Materiali da Consegnaree; e (b) ha vincolato i propri dipendenti ad obblighi di riservatezza che impongono a tali dipendenti di utilizzare e divulgare i Dati Kyndryl solo quando i presenti Termini lo consentano.

3. Restituzione o Cancellazione dei Dati Kyndryl

3.1. Il Fornitore, a discrezione di Kyndryl, eliminerà o restituirà i Dati Kyndryl al termine o alla scadenza del Documento d'Ordine o anche prima su richiesta di Kyndryl. Se Kyndryl richiede la cancellazione, il Fornitore, in linea con le Migliori Pratiche del Settore, renderà i dati illeggibili ed impossibili da riassemblare o ricostruire e certificherà la cancellazione a Kyndryl. Se Kyndryl richiede la restituzione dei Dati Kyndryl, il Fornitore procederà in tal senso attenendosi ad una tempificazione ragionevole di Kyndryl e seguendo le ragionevoli istruzioni scritte di Kyndryl.

Articolo III, Privacy

Questo Articolo si applica se il Fornitore Tratta Dati Personali di Kyndryl.

1. Trattamento dei Dati Personali

1.1 Kyndryl nomina il Fornitore come Responsabile del Trattamento dei Dati Personali di Kyndryl al solo scopo di fornire i Materiali da Consegnare e i Servizi in conformità con le istruzioni di Kyndryl, incluse quelle contenute nei presenti Termini, nel Documento d'Ordine e nel relativo accordo base tra le parti. Nel caso in cui il Fornitore non possa attenersi ad un'istruzione, Kyndryl potrà recedere parzialmente dalla parte di Servizio coinvolta, inviando al Fornitore un preavviso scritto. Qualora il Fornitore ritenga che un'istruzione violi una legge sulla protezione dei dati, il Fornitore informerà immediatamente Kyndryl entro il periodo di tempo previsto per legge.

1.2 Il fornitore si atterrà a tutte le leggi sulla protezione dei dati applicabili ai Servizi ed ai Materiali da Consegnare.

1.3 Un'Appendice al Documento d'Ordine, o lo stesso Documento d'Ordine, stabiliscono quanto segue in relazione ai Dati Kyndryl:

(a) le categorie di Interessati;
(b) le categorie di Dati Personali di Kyndryl;
(c) azioni sui dati e attività di Trattamento;
(d) durata e frequenza del Trattamento; e
(e) un elenco di Subresponsabili.

2. Misure Tecniche e Organizzative (TOMs)

2.1 Il Fornitore implementerà e seguirà le misure tecniche e organizzative stabilite nell'Articolo II (Misure Tecniche e Organizzative, Sicurezza dei dati) e nell'Articolo VIII (Misure Tecniche e Organizzative, Sicurezza Generale) in tal modo garantendo un livello di sicurezza adeguato al rischio presentato dai propri Servizi e Materiali da Consegnare. Il Fornitore certifica e comprende le limitazioni di cui all'Articolo II, al presente Articolo III e all'articolo VIII e le rispetterà.

3. Diritti e Richieste degli Interessati

3.1 Il Fornitore informerà tempestivamente Kyndryl (in tempi che consentano a Kyndryl e agli Altri Titolari del Trattamento dei Dati Personali di adempiere alle proprie obbligazioni legali) di qualsiasi richiesta da parte di un Interessato di esercitare i propri diritti (ad es. rettifica, cancellazione o blocco dei dati) in merito ai Dati Personali di Kyndryl. Il Fornitore può anche indirizzare prontamente un Interessato ad inviare la richiesta a Kyndryl. Il Fornitore non risponderà ad alcuna richiesta da parte degli Interessati, a meno che non sia legalmente richiesto o richiesto da Kyndryl per iscritto.

3.2 Se Kyndryl è obbligata a fornire informazioni in merito ai Dati Personali di Kyndryl ad Altri Titolari del Trattamento dei Dati Personali o a terze parti (ad esempio, Interessati o regolatori), il Fornitore assisterà Kyndryl fornendo informazioni e intraprendendo le ragionevoli azioni richieste da Kyndryl, con un programma che consenta ad Kyndryl di rispondere tempestivamente a tali Altri Titolari del Trattamento dei Dati Personali o terze parti.

4. Subresponsabili

4.1 Il Fornitore darà a Kyndryl un preavviso scritto prima di aggiungere un nuovo Subresponsabile o prima di ampliare l'ambito di Trattamento di un Subresponsabile esistente, riportando in tale comunicazione scritta il nome del Subresponsabile e descrivendo il nuovo o ampliato ambito di Trattamento. Kyndryl potrà opporsi a qualsiasi nuovo Subresponsabile o ambito ampliato per motivi ragionevoli in qualsiasi

momento e, in tal caso, le parti lavoreranno insieme in buona fede per gestire l'obiezione di Kyndryl. Fatto salvo il diritto di Kyndryl di opporsi in qualsiasi momento, il Fornitore potrà ingaggiare il nuovo Subresponsabile o espandere l'ambito di Trattamento del Subresponsabile esistente nel caso Kyndryl non sollevi obiezioni entro 30 giorni dalla data della comunicazione scritta da parte del Fornitore.

4.2 Il Fornitore imporrà le obbligazioni di protezione, sicurezza e certificazione dei dati stabiliti nei presenti Termini a ciascun Subresponsabile prima che un Subresponsabile Tratti i Dati Kyndryl. Il Fornitore è pienamente responsabile nei confronti di Kyndryl per l'adempimento delle obbligazioni di ciascun Subresponsabile.

5. Trattamento dei Dati Transfrontaliero

Per come vengono utilizzati di seguito:

Paese Adeguato indica un paese che fornisce un livello adeguato di protezione dei dati riguardo il relativo trasferimento ai sensi delle normative applicabili sulla protezione dei dati o in base alle decisioni di organismi regolatori.

Importatore di Dati indica un Responsabile del Trattamento o un Subresponsabile che non si trova in un Paese Adeguato.

SCC UE (EU Standard Contractual Clauses) indica le Clausole Contrattuali Standard UE (Commission Decision 2021/914) con l'applicazione delle clausole opzionali, ad eccezione dell'opzione 1 della Clausola 9(a) e dell'opzione 2 della Clausola 17, ufficialmente pubblicate alla pagina https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en.

Serbian Standard Contractual Clauses ("Serbian SCCs")india le Clausole Contrattuali Standard della Serbia come adottate dalla "Serbian Commissioner for Information of Public Importance and Personal Data Protection", pubblicate alla pagina https://www.poverenik.rs/images/stories/dokumentacija-nova/podzakonski-akti/Klauzulelat.docx.

SCCs (**Standard Contractual Clauses**) indica le clausole contrattuali richieste dalle leggi sulla protezione dei dati applicabili per il trasferimento di Dati personali a Responsabili del Trattamento che non sono stabiliti in Paesi Adeguati.

United Kingdom International Data Transfer Addendum to the EU Commission Standard Contractual Clauses ("UK Addendum") indica l'Appendice sul trasferimento internazionale di dati del Regno Unito alle clausole contrattuali standard della commissione europea, come pubblicato ufficialmente alla pagina https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-Transfer-agreement-and-guidance/.

L'Addendum per la Svizzera alle Clausole Contrattuali Standard della Commissione europea ("Addendum per la Svizzera") indica le clausole contrattuali alle Clausole Contrattuali Standard della Commissione europea che si applicano in conformità alla decisione dell'Autorità per la protezione dei dati della Svizzera (**"FDPIC"**) ed in conformità alla Legge federale svizzera sulla Protezione dei dati (Federal Act on Data Protection, **"FADP"**).

5.1 Il Fornitore non trasferirà o divulgherà (neanche mediante accesso remoto) senza il previo consenso scritto di Kyndryl alcun Dato Personale di Kyndryl oltre i confini. Se Kyndryl fornisce tale consenso, le parti collaboreranno per garantire il rispetto delle leggi applicabili sulla protezione dei dati. Se da tali leggi sono richieste le SCCs, il Fornitore si adeguerà prontamente su richiesta di Kyndryl alle SCCs.

5.2 In relazione alle SCCs UE:

(a) Se il Fornitore non è stabilito in un Paese Adeguato: con la presente il Fornitore sta stipulando in proprio conto le SCCs UE con Kyndryl come Importatore di Dati e il Fornitore stipulerà accordi scritti con ciascun Subresponsabile approvato, in conformità con la Clausola 9 delle SCCs UE, e fornirà su richiesta a Kyndryl le copie di tali accordi.

(i) Il Modulo 1 delle SCCs UE non si applica se non diversamente concordato per iscritto dalle parti.

(ii) Il Modulo 2 delle SCCs US si applica nei casi in cui Kyndryl è Titolare del Trattamento dei Dati ed il Modulo 3 si applica nei casi in cui Kyndryl è Responsabile del Trattamento dei Dati. In base alla Clausola 13 delle SCCs UE, quando si applicano i Moduli 2 o 3, le parti concordano che (1) le SCCs UE saranno disciplinate dalla legge dello stato membro dell'UE in cui ha sede l'autorità di controllo competente e (2) qualsiasi controversia derivante dalle SCCs UE sarà giudicata nei tribunali dello stato membro dell'UE in cui ha sede l'autorità di controllo competente. Se tale normativa in (1) non consente diritti di beneficiari di terze parti, le SCCs UE sarano disciplinate dalle leggi dei Paesi Bassi e tutte le controversie derivanti dalle SCCs UE ai sensi di (2) saranno risolte dal Tribunale di Amsterdam nei Paesi Bassi.

(b) Se il Fornitore ha sede nello Spazio Economico Europeo e Kyndryl è un Titolare del Trattamento dei Dati non soggetto al General Data Protection Regulation 2016/679, si applica il Modulo 4 delle SCC UE e il Fornitore, con la presente, sta stipulando le SCC UE con Kyndryl come esportatore di dati. Se si applica il Modulo 4 delle SCC UE, le parti concordano che le SCCs UE saranno disciplinate dalle leggi dei Paesi Bassi e che tutte le controversie derivanti dalle SCCs UE saranno risolte dal Tribunale di Amsterdam nei Paesi Bassi.

(c) Qualora gli Altri Titolari del Trattamento dei Dati Personali, quali Clienti o affiliate, richiedano di diventare parte delle SCCs UE ai sensi della "clausola di docking" di cui alla clausola 7, il Fornitore con la presente accetta tale richiesta.

(d) Le Misure Tecniche e Organizzative (TOMs) necessarie per completare l'Allegato II delle SCCs UE possono essere trovate nei presenti Termini, nel Documento d'Ordine stesso e nel relativo accordo base tra le parti.

(e) In caso di conflitto tra le SCCs UE ed i presenti Termini, prevarranno le SCCs UE.

5.3 In relazione alle UK SCCs:

(a) Se il Fornitore non è stabilito in un Paese Adeguato: (i) con la presente il Fornitore sta stipulando in proprio conto le UK SCCs con Kyndryl come Importatore di Dati; e (ii) il Fornitore stipulerà accordi scritti con ciascun Subresponsabile approvato che sia un Importatore di Dati, in conformità con la Clausola 11 delle UK SCCs, e fornirà su richiesta a Kyndryl copie di tali accordi.

(b) Se il Fornitore è stabilito in un Paese Adeguato, con la presente il Fornitore stipula accordi UK SCCs con Kyndryl in nome e per conto di ciascun Subresponsabile che sia un Importatore di Dati. Se il Fornitore non è in grado di farlo per tali Subresponsabili, allora, prima di consentire al Subresponsabile di Trattare i Dati Personali di Kyndryl, fornirà a Kyndryl le UK SCCs firmate da tale Subresponsabile per la controfirma da parte di Kyndryl.

(c) Le UK SCCs tra Kyndryl e il Fornitore fungeranno da UK SCCs tra un Titolare del Trattamento dei Dati ed il Responsabile del Trattamento o come un accordo scritto back-to-back tra "importatore di dati" e "subresponsabile" in conformità con la clausola 11 delle UK SCCs, come richiesto dai fatti. In caso di conflitto tra le UK SCCs ed i presenti Termini, prevarranno le UK SCCs.

(d) Altri Titolari del Trattamento dei Dati, quali i Clienti o le affiliate, possono richiedere di diventare ulteriori "esportatori di dati". Con la presente il Fornitore acconsente per proprio conto e per conto dei propri Subresponsabili a tale richiesta. Kyndryl informerà il Fornitore di eventuali ulteriori "esportatori di dati" e, a sua volta, il Fornitore informerà i propri Subresponsabili che sono Importatori di Dati di tali ulteriori "esportatori di dati".

5.4 In merito al/gli UK Addendum:

a) Se il Fornitore non ha sede in un Paese Adeguato: (i) con la presente il Fornitore aderisce allo/agli UK Addendum con Kyndryl come Importatore da allegare alle EU SCC illustrate in precedenza (ove applicabile, a seconda delle circostanze delle attività di trattamento); e (ii) il Fornitore stipulerà accordi scritti con ciascun Subresponsabile approvato e fornirà, su richiesta, a Kyndryl copie di tali accordi.

b) Se il Fornitore ha sede in un Paese Adeguato e Kindryl è Titolare del trattamento dei dati non soggetto al UK General Data Protection Regulation (quale integrato nella legge del Regno Unito ai sensi dello European Union (Withdrawal) Act 2018), con la presente il Fornitore stipula lo/gli UK Addendum come Esportatore con Kyndryl, da allegare alle EU SCC indicate nel precedente paragrafo 5.2(b).

c) Se altri titolari del trattamento dei dati, quali i Clienti o le affiliate, richiedono di diventare parte contraente dello/degli UK Addendum, con la presente il Fornitore acconsente a tale richiesta.

d) Le Informazioni di Appendice (come indicato nella Tabella 3) nello/negli UK Addendum sono disponibili nelle EU SCC applicabili, nei presenti Termini, nello stesso Documento di Transazione e nel relativo accordo di base tra le parti. Né Kyndryl né il Fornitore possono risolvere lo/gli UK Addendum quando l'UK Addendum cambia.

e) In caso di conflitto tra lo/gli UK Addendum e i presenti Termini, lo/gli UK Addendum prevarrà/anno.

5.5 In relazione alle Serbian SCCs:

(a) Se il Fornitore non è stabilito in un Paese Adeguato: (i) con la presente il Fornitore sta stipulando in proprio conto le Serbian SCCs con Kyndryl come Responsabile del Trattamento dei Dati; e (ii) il Fornitore stipulerà accordi scritti con ciascun Subresponsabile approvato, in conformità con l'Articolo 8 delle Serbian SCCs, e fornirà su richiesta a Kyndryl copie di tali accordi.

(b) Se il Fornitore è stabilito in un Paese Adeguato, con la presente il Fornitore stipula accordi Serbian SCCs con Kyndryl in nome e per conto di ciascun Subresponsabile ubicato in un Paese Non Adeguato. Se il Fornitore non è in grado di farlo per tali Subresponsabili, allora, prima di consentire al Subresponsabile di Trattare i Dati Personali di Kyndryl, fornirà a Kyndryl le Serbian SCCs firmate da tale Subresponsabile per la controfirma da parte di Kyndryl.

(c) Le Serbian SCCs tra Kyndryl e il Fornitore fungeranno da Serbian SCCs tra un Titolare del Trattamento dei Dati ed il Responsabile del Trattamento o come un accordo scritto back-to-back tra "responsabile del trattamento" e "subresponsabile", come richiesto dai fatti. In caso di conflitto tra le Serbian SCCs ed i presenti Termini, prevarranno le Serbian SCCs.

(d) Le Informazioni necessarie per completare le Appendici dalla 1 alla 8 delle Serbian SCCs ai fini della regolamentazione del trasferimento di Dati Personali in un Paese Non Adeguato sono reperibili nei presenti Termini e nell'Appendice del Documento d'Ordine o nel Documento d'Ordine stesso.

5.6 In relazione all'Addendum/agli Addenda per la Svizzera:

(a) Qualora e nella misura in cui un trasferimento di Dati Personali di Kyndryl ai sensi del paragrafo 5.1. sia soggetto alla Legge federale svizzera sulla protezione dei dati (Federal Act on Data Protection, "FADP"), le SCC dell'UE concordate nel paragrafo 5.2. dei presenti Termini regoleranno il trasferimento, con le seguenti modifiche per il recepimento dello standard GDPR per i Dati personali svizzeri:

- i riferimenti al Regolamento Generale sulla Protezione dei Dati ("GDPR") devono essere intesi anche come riferimenti alle disposizioni equivalenti del FADP,
- la Swiss Federal Data Protection Information Commission è l'autorità di controllo competente, ai sensi della Clausola 13 e dell'Allegato I.C delle SCC dell'UE
- la legislazione svizzera è la legge applicabile nel caso in cui il trasferimento sia soggetto esclusivamente al FADP e
- il termine "stato membro" nella Clausola 18 delle SCC dell'UE sarà esteso per includere la Svizzera, allo scopo di consentire agli Interessati svizzeri di esercitare i propri diritti nel loro luogo di residenza abituale.

(b) Per fugare ogni dubbio, nulla di quanto sopra ha lo scopo di ridurre in alcun modo il livello di protezione dei dati fornito dalle SCC dell'UE, ma solo di estendere tale livello di protezione agli Interessati svizzeri. Se e nella misura in cui ciò non avvenga, prevarranno le disposizioni delle SCC dell'UE.

6. Assistenza e Registro

6.1 Tenendo conto della natura del Trattamento, il Fornitore assisterà Kyndryl adottando misure tecniche e organizzative adeguate ad adempiere alle obbligazioni associate alle richieste e ai diritti dell'Interessato. Il Fornitore assisterà inoltre Kyndryl nel garantire il rispetto delle obbligazioni relative alla sicurezza del Trattamento, la notifica e la comunicazione di una Violazione della Sicurezza e la creazione di valutazioni di impatto sulla protezione dei dati, compresa la consultazione preventiva con l'autorità di regolamentazione responsabile, se necessaria, tenendo conto delle informazioni disponibili al Fornitore.

6.2 Il Fornitore manterrà un registro aggiornato del nome e dei dettagli di contatto di ciascun Subresponsabile, inclusi i rappresentanti di ciascun Subresponsabile e il responsabile della protezione dei dati. Su richiesta, il Fornitore darà questo registro a Kyndryl secondo un programma che consentirà a Kyndryl di rispondere tempestivamente a qualsiasi richiesta da parte di un Cliente o di terze parti.

Articolo IV, Misure Tecniche e Organizzative (TOMs), Sicurezza del Codice

Questo Articolo si applica se il Fornitore ha accesso al Codice Sorgente Kyndryl. Il Fornitore si atterrà ai requisiti del presente Articolo e, in tal modo, proteggerà il Codice Sorgente Kyndryl da perdita, distruzione, alterazione, divulgazione accidentale o non autorizzata, accesso accidentale o non autorizzato e forme illecite di Gestione. I requisiti di questo Articolo si estendono a tutte le applicazioni, piattaforme e infrastrutture IT su cui il fornitore opera o che gestisce durante la fornitura dei Materiali da Consegnare e dei Servizi e nella Gestione della Tecnologia IT, inclusi tutti gli ambienti operativi di sviluppo, test, hosting, supporto ed i data center.

1. Requisiti di Sicurezza

Per come utilizzati di seguito,

Paese Interdetto indica qualsiasi paese: (a) che il governo degli Stati Uniti ha designato come foreign adversary (avversario straniero) ai sensi dell'Ordine Esecutivo del 15 maggio 2019 Securing the Information and Communications Technology and Services Supply Chain, (b) elencato in conformità con l'articolo 1654 dello U.S. National Defense Authorization Act of 2019, o (c) identificato come "Paese Interdetto" nel Documento d'Ordine.

1.1. Il fornitore non distribuirà né inserirà alcun Codice Sorgente Kyndryl in deposito a garanzia di terzi.

1.2. Il Fornitore non consentirà che alcun Codice Sorgente Kyndryl risieda su server situati in un Paese Interdetto. Il Fornitore non consentirà a nessuno, incluso il proprio Personale, situato in un Paese Interdetto o in visita in un Paese Interdetto (per la durata di tale visita), per qualsiasi motivo, di accedere o utilizzare qualsiasi Codice Sorgente Kyndryl, indipendentemente dal luogo in cui tale Codice Sorgente Kyndryl sia localizzato a livello globale, e il Fornitore non consentirà lo sviluppo, il test o altre attività che richiederebbero tale accesso o utilizzo in un Paese Interdetto.

1.3. Il Fornitore non inserirà o distribuirà il Codice Sorgente Kyndryl in alcuna giurisdizione in cui la legge o l'interpretazione della legge richieda la divulgazione del Codice Sorgente a terzi. Se si verifica un cambiamento di legge o dell'interpretazione della legge in una giurisdizione in cui si trova il Codice Sorgente Kyndryl che potrebbe comportare l'obbligo per il Fornitore di divulgare tale Codice Sorgente a terzi, il Fornitore distruggerà immediatamente o rimuoverà immediatamente tale codice Sorgente Kyndryl da tale giurisdizione e non inserirà alcun Codice Sorgente Kyndryl aggiuntivo in tale giurisdizione fintanto che tale legge o interpretazione della legge rimane operativa.

1.4. Il Fornitore non intraprenderà, direttamente o indirettamente, alcuna azione, inclusa la stipula di alcun accordo, che induca il Fornitore, Kyndryl o terzi a incorrere in un obbligazione di divulgazione ai sensi degli artt. 1654 o 1655 del National Defense Authorization Act del 2019. Per chiarezza, salvo quanto espressamente consentito nel Documento d'Ordine o nell'accordo base associato tra le parti, al Fornitore non è consentito divulgare il Codice Sorgente Kyndryl a terzi, in qualsiasi circostanza, senza il previo consenso scritto di Kyndryl.

1.5. Se Kyndryl notifica al Fornitore o una terza parte notifica a una delle parti che: (a) Il Fornitore ha consentito che il Codice Sorgente Kyndryl fosse portato in un Paese Interdetto o in qualsiasi giurisdizione soggetta al precedente Articolo 1.3, (b) il Fornitore ha altrimenti rilasciato, effettuato accesso o utilizzato il Codice Sorgente Kyndryl in un modo non consentito dal Documento d'Ordine o dall'accordo base associato o da altri accordi tra le parti o (c) il Fornitore ha violato l'Articolo 1.4 di cui sopra, quindi senza limitare i diritti di Kyndryl di rimediare a tale non conformità legale o patrimoniale o ai sensi del Documento d'Ordine o dell'accordo base associato o di altri accordi tra le parti: (i) se tale notifica è rivolta al Fornitore, il Fornitore condividerà prontamente la notifica con Kyndryl; e (ii) il Fornitore, secondo la ragionevole direzione di Kyndryl, indagherà e risolverà la questione secondo il programma che Kyndryl ragionevolmente determinerà (previa consultazione con il Fornitore).

1.6. Se Kyndryl ritiene ragionevolmente che siano necessari dei cambiamenti nelle politiche, procedure, controlli o pratiche del Fornitore in relazione all'accesso al Codice Sorgente per gestire la sicurezza informatica, il furto di proprietà intellettuale o rischi simili o correlati (incluso il rischio che senza tali cambiamenti Kyndryl possa vedere applicate limitazioni alla vendita a determinati Clienti o in determinati mercati o potrebbe essere altrimenti incapace di soddisfare i requisiti di sicurezza del Cliente

o della supply chain), Kyndryl potrà contattare il Fornitore per discutere le azioni necessarie per far fronte a tali rischi, comprese le modifiche a tali politiche, procedure, controlli o pratiche. Su richiesta di Kyndryl, il Fornitore collaborerà con Kyndryl nella valutazione della necessità di tali modifiche e nell'implementazione di modifiche appropriate e reciprocamente concordate.

Articolo V, Sviluppo Sicuro

Il presente Articolo si applica se il Fornitore fornirà il Codice Sorgente o il Software On-Premise propri o di terze parti a Kyndryl, oppure se i Servizi o i Materiali da Consegnare del Fornitore saranno forniti ad un Cliente Kyndryl come parte di un prodotto o servizio Kyndryl.

1. Livello di adeguatezza della Sicurezza

Il Fornitore collaborerà nei processi interni di Kyndryl che valutano il livello di adeguatezza della sicurezza dei prodotti e servizi Kyndryl che dipendono da uno qualsiasi dei Materiali da Consegnare del Fornitore, anche rispondendo tempestivamente e pienamente alle richieste di informazioni, attraverso documenti, altri registri, colloqui con il Personale del Fornitore, o simili.

2. Sviluppo Sicuro

2.1 Il presente Articolo 2 si applica solo nel caso in cui il Fornitore fornisca Software On-Premise a Kyndryl.

2.2 Il Fornitore ha implementato e manterrà, in conformità con le Best Practice del settore, per tutta la durata contrattuale definita nel Documento d'Ordine, la rete, la piattaforma, il sistema, l'applicazione, il dispositivo, l'infrastruttura fisica, la procedura di risposta agli incidenti e le politiche, le procedure e i controlli di sicurezza incentrati sul Personale necessari a proteggere: (a) lo sviluppo, il build, il test e i sistemi operativi e gli ambienti che il Fornitore o qualsiasi terza parte incaricata dal Fornitore gestisce, utilizza o su cui fa affidamento in altro modo per o in relazione ai Materiali da Consegnare e (b) tutti i codici sorgente dei Materiali da Consegnare contro la perdita, forme illecite di gestione e accesso, divulgazione o alterazione non autorizzati.

3. Vulnerabilità delle Sicurezza

3.1 Il presente Articolo 3 si applica solo se i Servizi o i Materiali da Consegnare del Fornitore saranno forniti ad un Cliente Kyndryl come parte di un prodotto o servizio Kyndryl.

3.2 Il Fornitore otterrà una certificazione di conformità a ISO 20243, Information Technology, Open Trusted Technology Provider, TM Standard (O-TTPS), Mitigazione di prodotti contaminati e contraffatti (o una certificazione autovalutata o certificazione basata sulla valutazione di un revisore indipendente affidabile). In alternativa, dopo richiesta per iscritto del Fornitore e relativa approvazione per iscritto di Kyndryl, il Fornitore otterrà una certificazione di conformità con uno standard di settore sostanzialmente equivalente che s'interessa dello sviluppo sicuro e delle pratiche della supply chain (o una certificazione autovalutata o certificazione basata sulla valutazione di un revisore indipendente affidabile, se e quando approvata da Kyndryl).

3.3 Il Fornitore otterrà la certificazione di conformità alla ISO 20243 o ad uno standard di settore sostanzialmente equivalente (se Kyndryl lo approva per iscritto) entro 180 giorni dalla data di entrata in vigore del presente Documento d'Ordine e rinnoverà tale certificazione successivamente ogni 12 mesi (ogni rinnovo dovrà essere effettuato nel rispetto della versione più recente degli standard applicabili, ossia ISO 20243 o, se Kyndryl approva per iscritto, uno standard di settore sostanzialmente equivalente che definisca le pratiche da implementare per uno sviluppo sicuro e per la supply chain).

3.4 Il Fornitore, su richiesta, fornirà tempestivamente a Kyndryl una copia delle certificazioni che lo stesso è tenuto ad ottenere, secondo gli Artt. 2.1 e 2.2 di cui sopra.

4. Vulnerabilità delle Sicurezza

Per come utilizzati di seguito,

Correzione degli Errori si intendono correzioni e verifiche di bug che correggono errori o carenze, comprese Vulnerabilità della Sicurezza, nei Materiali da Consegnare.

Mitigazione indica qualsiasi mezzo noto per ridurre o evitare i rischi di una Vulnerabilità della Sicurezza.

Vulnerabilità della Sicurezza indica uno stato nella progettazione, codifica, sviluppo, implementazione, test, operatività, supporto, manutenzione o gestione del Materiali da Consegnare che consenta un attacco da parte di chiunque che possa comportare accessi o sfruttamenti non autorizzati, incluso: (a) accesso, controllo o interruzione del funzionamento di un sistema, (b) accesso a, eliminazione, alterazione o estrazione di dati o (c) cambiamenti di identità, autorizzazioni o permessi di utenti o amministratori. Una Vulnerabilità della Sicurezza può esistere indipendentemente dal fatto che gli siano stati assegnati un ID CVE (Common Vulnerabilities and Exposures) o qualsiasi punteggio o classificazione ufficiale.

4.1 Il Fornitore dichiara e garantisce che provvederà a: (a) mettere in atto le Migliori Pratiche del Settore per identificare le Vulnerabilità della Sicurezza, anche attraverso la continua scansione della sicurezza delle applicazioni con codice sorgente statico e dinamico, scansione della sicurezza del codice open source e scansione delle vulnerabilità del sistema, e (b) rispettare i requisiti dei presenti Termini per aiutare a prevenire, rilevare e correggere le Vulnerabilità della Sicurezza nei Materiali da Consegnare e in tutte le applicazioni, piattaforme e infrastrutture della IT attraverso le quali il Fornitore crea ed eroga Servizi e Materiali da Consegnare.

4.2 Se il Fornitore viene a conoscenza di una vulnerabilità legata alla sicurezza dei Materiali da Consegnare o in tali applicazioni, piattaforme o infrastrutture IT, il Fornitore fornirà a Kyndryl una Correzione degli Errori e Mitigazioni per tutte le versioni e le release dei Materiali da Consegnare in conformità con i Livelli di Gravità e gli intervalli di tempo definiti nelle seguenti tabelle:

Livello di Gravità*
Vulnerabilità della Sicurezza di Emergenza – una Vulnerabilità della Sicurezza che costituisce una grave e potenziale minaccia globale. Kyndryl designa le Vulnerabilità della Sicurezza di Emergenza a sua esclusiva discrezione, indipendentemente dal Punteggio di Base CVSS.
Critica – rappresenta un Vulnerabilità della Sicurezza con Punteggio di Base CVSS che varia da 9 a 10,0.
Alta – rappresenta un Vulnerabilità della Sicurezza con Punteggio di Base CVSS che varia da 7,0 a 8,9.
Media – rappresenta un Vulnerabilità della Sicurezza con Punteggio Base CVSS che varia da 4,0 a 6,9.
Bassa – rappresenta un Vulnerabilità della Sicurezza con Punteggio Base CVSS che varia da 0,0 a 3,9.

Intervalli di Tempo				
Emergenza	***Critica***	***Alto***	***Media***	***Basso***
4 Giorni o meno, come determinato dal Chief Information Security Office di Kyndryl	30 Giorni	30 Giorni	90 Giorni	In base alle Migliori Pratiche del Settore

* In qualsiasi caso in cui una Vulnerabilità della Sicurezza non abbia un Punteggio di Base CVSS prontamente assegnato, il Fornitore applicherà un Livello di Gravità appropriato per la natura e le circostanze di tale vulnerabilità.

4.3 Per una Vulnerabilità della Sicurezza divulgata pubblicamente e per la quale il Fornitore non abbia ancora fornito a Kyndryl alcuna Mitigazione o Correzione degli Errori, il Fornitore implementerà tutti controlli di sicurezza aggiuntivi tecnicamente fattibili atti a mitigare i rischi derivanti dalla vulnerabilità.

4.4 Se Kyndryl non è soddisfatta della risposta del Fornitore ad una qualsiasi Vulnerabilità della Sicurezza presente in uno dei Materiali da Consegnare o in una qualsiasi delle applicazioni, piattaforme o infrastrutture di cui sopra, fatti salvi eventuali altri diritti di Kyndryl, il Fornitore si organizzerà tempestivamente affinché Kyndryl possa discutere delle proprie preoccupazioni direttamente con un Vice Presidente del Fornitore o con un dirigente equivalente, responsabile dell'erogazione della Correzione degli Errori.

4.5 Esempi di Vulnerabilità della Sicurezza includono i casi in cui il codice di terze parti o il codice open

source di fine servizio (EOS) che non riceve più correzioni di sicurezza.

Articolo VI, Accesso ai Sistemi Aziendali

Questo Articolo si applica se i dipendenti del Fornitore avranno accesso ad un qualsiasi Sistema Aziendale.

1. Termini Generali

1.1 Kyndryl determinerà se autorizzare i dipendenti del fornitore ad accedere ai sistemi aziendali. Se Kyndryl lo autorizza, il Fornitore si rispetterà e farà anche in modo che i propri dipendenti con tale accesso rispettino i requisiti di questo Articolo.

1.2 Kyndryl identificherà i mezzi con cui i dipendenti del Fornitore potranno accedere ai Sistemi Aziendali, incluso se tali dipendenti accederanno ai Sistemi Aziendali tramite Dispositivi forniti da Kyndryl o dal Fornitore.

1.3 Per erogare i Servizi i Dipendenti del Fornitore potranno accedere unicamente ai Sistemi Aziendali e potranno utilizzare solo i Dispositivi autorizzati da Kyndryl per tale accesso. I dipendenti del Fornitore non possono utilizzare i Dispositivi così autorizzati da Kyndryl per fornire servizi a qualsiasi altra persona o entità, o per accedere a sistemi IT, reti, applicazioni, siti Web, strumenti di posta elettronica, strumenti di collaborazione o simili o in connessione con i Servizi del Fornitore o di terze parti.

1.4 Per chiarezza, i dipendenti del Fornitore non possono utilizzare i Dispositivi che Kyndryl autorizza per accedere ai Sistemi Aziendali per qualsiasi motivo personale (ad esempio, i dipendenti del Fornitore non potranno archiviare file personali come musica, video, immagini o altri elementi simili su tali Dispositivi e non potranno utilizzare Internet da tali Dispositivi per motivi personali).

1.5 I dipendenti del Fornitore non copieranno il Materiale Kyndryl accessibile tramite un Sistema Aziendale senza la previa approvazione scritta di Kyndryl (e non copieranno mai il Materiale Kyndryl su un dispositivo di archiviazione portatile, come un dispositivo USB, un disco rigido esterno o altri oggetti simili).

1.6 Su richiesta, il Fornitore confermerà, in base al nome del dipendente, i sistemi aziendali specifici ai quali i propri dipendenti sono autorizzati ad accedere e a cui hanno avuto accesso, in qualsiasi periodo di tempo identificato da Kyndryl.

1.7 Il Fornitore informerà Kyndryl entro ventiquattro (24) ore che un dipendente del Fornitore con accesso a qualsiasi Sistema Aziendale non è più: (a) dipendente del Fornitore o (b) impegnato in attività che richiedano tale accesso. Il Fornitore collaborerà con Kyndryl per garantire che l'accesso per tali dipendenti precedenti o attuali venga immediatamente revocato.

1.8 Il Fornitore a Kyndryl segnalerà immediatamente eventuali incidenti di sicurezza effettivi o sospetti (quali ad esempio la perdita di un Dispositivo Kyndryl o del Fornitore o l'accesso non autorizzato a un Dispositivo o a dati, materiali o altre informazioni di qualsiasi tipo) e collaborerà con Kyndryl nelle indagini su tali incidenti.

1.9 Il Fornitore non può consentire ad alcun agente, appaltatore indipendente o dipendente del subappaltatore di accedere a qualsiasi Sistema Aziendale, senza il previo consenso scritto di Kyndryl; se Kyndryl fornisce tale consenso, il Fornitore impegnerà contrattualmente tali persone e i relativi datori di lavoro al rispetto dei requisiti del presente Articolo come se tali persone fossero dipendenti del Fornitore, e sarà responsabile nei confronti di Kyndryl per tutte le azioni e le omissioni ad agire di tale persona o datore di lavoro rispetto a tale accesso al Sistema Aziendale.

2. Software del Dispositivo

2.1 Il Fornitore richiederà ai propri dipendenti di installare tempestivamente tutto il software del Dispositivo richiesto da Kyndryl per assicurare un accesso sicuro ai Sistemi Aziendali. Né il Fornitore né i suoi dipendenti interferiranno con le operazioni di tale software o con le funzionalità di sicurezza abilitate dal software.

2.2 Il Fornitore ed i propri dipendenti si atterranno alle regole di configurazione del Dispositivo stabilite da Kyndryl e collaboreranno in altro modo con Kyndryl per garantire che il software funzioni come previsto da Kyndryl. Ad esempio, il Fornitore non sostituirà il blocco del sito Web del software o le funzionalità di patch automatizzate.

2.3 I dipendenti del Fornitore non potranno condividere con altre persone i Dispositivi che utilizzano per accedere ai Sistemi Aziendali, i relativi nomi utente, password o simili.

2.4 Se Kyndryl autorizza i dipendenti del Fornitore ad accedere ai Sistemi Aziendali utilizzando i Dispositivi del Fornitore, il Fornitore installerà ed eseguirà su tali Dispositivi un sistema operativo approvato da Kyndryl e aggiornerà a una nuova versione di tale sistema operativo o di un nuovo sistema operativo entro un tempo ragionevole dall'indicazione a fare ciò di Kyndryl.

3. Sorveglianza e Cooperazione

3.1 Kyndryl ha il diritto incondizionato per monitorare e porre rimedio a potenziali intrusioni e altre minacce alla sicurezza informatica in qualunque modo, da qualunque luogo e utilizzando qualsiasi mezzo che Kyndryl ritenga necessario o appropriato, senza preavviso al Fornitore, a qualsiasi dipendente del Fornitore o ad altri. Come esempi di tali diritti, Kyndryl potrà, in qualsiasi momento (a) eseguire un test di sicurezza su qualsiasi Dispositivo, (b) monitorare, ripristinare con mezzi tecnici o di altro tipo e verificare le comunicazioni (comprese le e-mail da qualsiasi account e-mail), i record, i file e altri elementi archiviati su qualsiasi Dispositivo o trasmessi attraverso qualsiasi Sistema Aziendale e (c) acquisire un'immagine forense completa di qualsiasi Dispositivo. Se Kyndryl necessita della collaborazione del Fornitore per esercitare i propri diritti, il Fornitore soddisferà pienamente e tempestivamente le richieste di Kyndryl per tale cooperazione (incluse, ad esempio, richieste di configurazione sicura di qualsiasi Dispositivo, installazione di software di monitoraggio o di altro tipo su qualsiasi Dispositivo, condivisione dei dettagli di connessione a livello di sistema, coinvolgimento nelle misure di risposta agli incidenti su qualsiasi Dispositivo e fornire ad Kyndryl accesso fisico a qualsiasi Dispositivo per ottenere un'immagine forense completa o altro e richieste simili e correlate).

3.2 Kyndryl potrà revocare l'accesso ai Sistemi Aziendali in qualsiasi momento, per qualsiasi dipendente del Fornitore o per tutti i dipendenti del Fornitore, senza preavviso al Fornitore, a qualsiasi dipendente del Fornitore o ad altri, se Kyndryl ritiene che ciò sia necessario per proteggere Kyndryl.

3.3 I diritti di Kyndryl non sono bloccati, diminuiti o limitati in alcun modo da alcuna disposizione del Documento d'Ordine, dall'accordo base associato tra le parti o da qualsiasi altro accordo tra le parti, inclusa qualsiasi disposizione che possa richiedere di ubicare dati, materiali o altre informazioni di qualsiasi tipo solo in una o più posizioni selezionate o che possa richiedere che solo le persone di una o più sedi selezionate accedano a tali dati, materiali o altre informazioni.

4. Dispositivi Kyndryl

4.1 Kyndryl manterrà il pieno titolo su tutti i Dispositivi Kyndryl, ed il Fornitore si farà carico del rischio di perdita dei Dispositivi, anche a causa di furto, vandalismo o negligenza. Il Fornitore non effettuerà né consentirà alcuna alterazione dei Dispositivi Kyndryl senza previo consenso scritto di Kyndryl, dove per alterazione si intende qualsiasi modifica ad un Dispositivo, inclusa qualsiasi modifica al software, alle applicazioni, alla progettazione della sicurezza, alla configurazione della sicurezza o alla progettazione fisica, meccanica o elettrica del Dispositivo.

4.2 Il Fornitore restituirà tutti i Dispositivi Kyndryl entro 5 giorni lavorativi dal termine della necessità di tali Dispositivi per l'erogazione dei Servizi e, se richiesto da Kyndryl, distruggerà contemporaneamente tutti i dati, materiali e altre informazioni di qualsiasi tipo presenti su tali Dispositivi, senza conservare alcuna copia, seguendo le Migliori Pratiche del Settore per cancellare definitivamente tutti questi dati, materiali e altre informazioni. Il Fornitore impacchetterà e restituirà, a proprie spese nel luogo identificato da Kyndryl, i Dispositivi Kyndryl nelle stesse condizioni in cui sono stati consegnati al Fornitore, a parte una ragionevole usura. La mancata osservanza da parte del Fornitore di qualsiasi obbligazione di cui al presente Articolo 4.2 costituisce una violazione sostanziale del Documento d'Ordine e del relativo accordo base e di qualsiasi accordo correlato tra le parti, con la consapevolezza che un accordo è "correlato" se l'accesso a qualsiasi Sistema Aziendale facilita le attività del Fornitore o altre attività ai sensi di tale accordo.

4.3 Kyndryl fornirà supporto per i Dispositivi Kyndryl (incluse l'ispezione e la manutenzione preventiva e correttiva dei Dispositivi). Il fornitore informerà tempestivamente Kyndryl della necessità di un servizio di rimedio.

4.4 Per i programmi software che Kyndryl possiede o su cui ha il diritto di licenza, Kyndryl concede al Fornitore un diritto temporaneo di utilizzare, archiviare e fare copie sufficienti per supportare il proprio utilizzo autorizzato dei Dispositivi Kyndryl. Il Fornitore non potrà trasferire programmi ad alcuno, fare copie delle informazioni sulla licenza del software o disassemblare, decompilare, decodificare o altrimenti tradurre qualsiasi programma se non espressamente consentito dalla legge applicabile senza incorrere in una deroga contrattuale.

5. L'Aggiornamento

5.1 Fermo restando quanto diversamente indicato nel Documento d'Ordine o in un accordo base associato tra le parti, previa comunicazione scritta al Fornitore e senza la necessità di ottenere il consenso del Fornitore, Kyndryl potrà aggiornare, integrare o altrimenti modificare il presente Articolo per soddisfare qualsiasi requisito ai sensi della legge applicabile o obbligazione del Cliente, per riflettere qualsiasi sviluppo delle migliori pratiche di sicurezza o altrimenti come Kyndryl ritiene necessario per proteggere i Sistemi Aziendali o Kyndryl.

Articolo VII, Incremento del Personale

Questo Articolo si applica nei casi in cui i dipendenti del Fornitore dedichino il proprio intero orario lavorativo all'erogazione dei Servizi per Kyndryl, forniscano tali Servizi presso i locali Kyndryl, i locali del Cliente o dalle proprie abitazioni ed eroghino i Servizi utilizzando unicamente i Dispositivi Kyndryl per accedere ai Sistemi Aziendali.

1. Accesso ai Sistemi Aziendali; Ambienti Kyndryl

1.1 Il Fornitore può eseguire i Servizi unicamente accedendo ai Sistemi Aziendali tramite i Dispositivi forniti da Kyndryl.

1.2 Per tutti gli accessi ai Sistemi Aziendali il Fornitore rispetterà i termini stabiliti nell'Articolo VI (Accesso ai Sistemi Aziendali).

1.3 I Dispositivi forniti da Kyndryl sono gli unici Dispositivi che il Fornitore e i propri dipendenti potranno utilizzare per erogare i Servizi e potranno essere utilizzati solo dal Fornitore e dai propri Dipendenti per erogare i Servizi. Per chiarezza, in nessun caso il Fornitore o i suoi dipendenti potranno utilizzare altri Dispositivi per erogare i Servizi o utilizzare i Dispositivi Kyndryl per qualsiasi altro cliente del Fornitore o per scopi diversi dall'erogazione di Servizi a Kyndryl.

1.4 I dipendenti dei Fornitori che utilizzano i Dispositivi Kyndryl potranno condividere il Materiale Kyndryl tra loro e archiviare tali materiali sui Dispositivi Kyndryl, ma solo finché tale condivisione e archiviazione si limitino alle sole attività necessarie ad eseguire con successo i Servizi.

1.5 Ad eccezione di tale archiviazione all'interno dei Dispositivi Kyndryl, in nessun caso il Fornitore o i suoi dipendenti potranno rimuovere alcun Materiale Kyndryl dai repository, dagli ambienti, dai tool o dalle infrastrutture Kyndryl in cui gli stessi sono conservati da Kyndryl.

1.6 Per chiarezza, il Fornitore e i suoi dipendenti non sono autorizzati a trasferire alcun Materiale Kyndryl su repository, ambienti, strumenti o infrastrutture del Fornitore o altri sistemi, piattaforme, reti o simili del Fornitore, senza il previo consenso scritto di Kyndryl.

1.7 L'Articolo VIII (Misure Tecniche e Organizzative, Sicurezza Generale) non si applica ai Servizi del Fornitore in cui i dipendenti del Fornitore dedichino il proprio intero orario lavorativo all'erogazione dei Servizi per Kyndryl, forniscano tali Servizi presso i locali Kyndryl, i locali del Cliente o dalle proprie abitazioni ed eroghino i Servizi utilizzando unicamente i Dispositivi Kyndryl per accedere ai Sistemi Aziendali. L'Articolo VIII si applica invece ai Servizi del Fornitore.

Articolo VIII, Misure Tecniche e Organizzative, Sicurezza Generale

Il presente Articolo si applica se il Fornitore offre Servizi o Materiali da Consegnare a Kyndryl, a meno che il Fornitore non abbia accesso alle sole BCI di Kyndryl durante l'erogazione di tali Servizi e Materiali da Consegnare (ossia, il Fornitore non elaborerà altri Dati Kyndryl o non avrà accesso ad alcun Materiale Kyndryl o Sistema Aziendale), se i Servizi e Materiali da Consegnare del Fornitore consistano solo nel fornire Software On-Premise a Kyndryl o se il Fornitore offre tutti i propri Servizi e Materiali da Consegnare sotto forma di incremento del personale ai sensi dell'Articolo VII, incluso l'Articolo 1.7.

Il Fornitore si atterrà ai requisiti del presente Articolo e in tal modo proteggerà: (a) i Materiali Kyndryl da perdita, distruzione, alterazione, divulgazione accidentale o non autorizzata e accesso accidentale o non autorizzato, (b) i Dati Kyndryl da forme illegali di Trattamento e (c) la Tecnologia Kyndryl da forme illegali di Gestione. I requisiti di questo Articolo si estendono a tutte le applicazioni, piattaforme e infrastrutture IT su cui il fornitore opera o che gestisce durante la fornitura dei Materiali da Consegnare e dei Servizi e nella Gestione della Tecnologia IT, inclusi tutti gli ambienti operativi di sviluppo, test, hosting, supporto ed i data center.

1. Policy di Sicurezza

1.1. Il Fornitore si atterrà alle policy e pratiche di sicurezza IT che sono parte integrante delle attività del Fornitore e obbligatorie per tutti i dipendenti del Fornitore e che rappresentano le Migliori Pratiche del Settore.

1.2. Il Fornitore verificherà le proprie policy e pratiche di sicurezza IT almeno una volta l'anno e le modificherà come egli ritiene necessario per proteggere il Materiale Kyndryl.

1.3. Il Fornitore si atterrà a tutti i requisiti inderogabili di legge relativi a tutte le nuove assunzioni ed estenderà tali requisiti a tutto il proprio Personale e a tutte le proprie consociate interamente controllate. Tali requisiti includeranno controlli sui precedenti penali secondo quanto consentito dalle leggi locali, prove di convalida dell'identità e qualsiasi controllo aggiuntivo che il Fornitore ritenga necessario. Il Fornitore ripeterà e convaliderà periodicamente questi requisiti, come ritiene necessario.

1.4. Il Fornitore terrà annualmente ai propri dipendenti corsi di formazione sulla sicurezza e la privacy e richiederà a tali dipendenti di certificare ogni anno il rispetto delle policy etiche di condotta commerciale, di riservatezza e di sicurezza del Fornitore, come stabilito nel codice di condotta del Fornitore o in documenti simili. Il Fornitore assicurerà una formazione aggiuntiva sulle policy e sui processi ai dipendenti con accesso amministrativo a tutti i componenti dei Servizi, dei Materiali da Consegnare e del Materiale Kyndryl. Tale formazione sarà specifica per il ruolo e mirata al supporto dei Servizi, dei Materiali da Consegnare e del Materiale Kyndryl e, in base alle esigenze, al rispetto della conformità e delle certificazioni richieste.

1.5. Il Fornitore dovrà definire misure di sicurezza e privacy per proteggere e garantire la disponibilità del Materiale Kyndryl, anche attraverso l'implementazione, manutenzione ed il rispetto della conformità alle policy e alle procedure che richiedono sicurezza e privacy attraverso una progettazione, una programmazione ed un'operatività protette, per tutti i Servizi ed i Materiali da Consegnare e per l'intera Gestione della Tecnologia Kyndryl.

2. Incidenti di Sicurezza

2.1. Il Fornitore manterrà e seguirà le politiche di risposta agli incidenti documentate conformi con le Migliori Pratiche del Settore per la gestione degli incidenti di sicurezza informatica.

2.2. Il fornitore esaminerà qualsiasi accesso o utilizzo non autorizzato del Materiale Kyndryl e definirà ed eseguirà un piano di risposta adeguato.

2.3. Il Fornitore informerà tempestivamente (e in ogni caso entro e non oltre 48 ore) Kyndryl dopo essere venuto a conoscenza di qualsiasi Violazione della Sicurezza. Il Fornitore effettuerà tale notifica a cyber.incidents@kyndryl.com. Il Fornitore consegnerà a Kyndryl le informazioni ragionevolmente richieste su tale violazione e sullo stato di qualsiasi attività di correzione e rimedio intrapresa dal Fornitore. A titolo di esempio, le informazioni ragionevolmente richieste possono includere log che dimostrino l'avvenuto accesso privilegiato, amministrativo e di altro tipo a Dispositivi, sistemi o applicazioni, immagini forensi di Dispositivi, sistemi o applicazioni e altri elementi simili, nella misura in cui ciò sia pertinente alla violazione o alle attività di ripristino e rimedio poste in essere dal Fornitore.

2.4. Il Fornitore offrirà a Kyndryl una ragionevole assistenza atta a soddisfare qualsiasi obbligazione legale (incluse le obbligazioni di notifica agli organismi di regolamentazione o agli interessati) di Kyndryl,

delle società affiliate e dei Clienti Kyndryl (e dei relativi clienti e società affiliate) in relazione a una Violazione della Sicurezza.

2.5. Il Fornitore non informerà o notificherà a terzi una Violazione della Sicurezza sia direttamente o indirettamente correlabile a Kyndryl a meno che Kyndryl non approvi ciò per iscritto o se richiesto dalla legge. Il Fornitore informerà Kyndryl per iscritto prima di distribuire qualsiasi notifica legalmente richiesta a terzi, laddove la notifica riveli direttamente o indirettamente l'identità di Kyndryl.

2.6. In caso di Violazione della Sicurezza derivante dalla violazione da parte del Fornitore di qualsiasi obbligazione ai sensi dei presenti Termini:

(a) Il Fornitore sarà responsabile di tutti i costi sostenuti, nonché dei costi effettivi sostenuti da Kyndryl, per la notifica della Violazione della Sicurezza agli organismi regolatori applicabili, ad altri enti governativi e organismi auto-regolamentati del settore, ai media (se richiesto dalla legge applicabile), agli Interessati, ai Clienti e ad altri,

(b) se Kyndryl lo richiede, il Fornitore, per 1 anno dalla data in cui tali Interessati sono stati informate della Violazione della Sicurezza, stabilirà e manterrà a proprie spese un call-center per rispondere alle domande degli Interessati in merito alla Violazione della Sicurezza e alle relative conseguenze, o secondo quanto richiesto da qualsiasi legge applicabile sulla protezione dei dati, a seconda di quale sia la protezione maggiore. Kyndryl e il Fornitore collaboreranno per redigere i testi e altri materiali che verranno utilizzati dal personale del call-center center per rispondere alle richieste. In alternativa, previa comunicazione scritta al Fornitore, Kyndryl potrà istituire e mantenere un proprio call-center center al posto del Fornitore e questi rimborserà a Kyndryl i costi effettivi sostenuti da Kyndryl per stabilire e mantenere tale call center, e

(c) il Fornitore rimborserà a Kyndryl i costi effettivi sostenuti da Kyndryl per fornire servizi di monitoraggio e di ripristino del credito per 1 anno dalla data in cui le persone colpite dalla violazione, che hanno scelto di registrarsi a tali servizi, sono state informate della Violazione della Sicurezza, o secondo quanto richiesto da qualsiasi legge applicabile sulla protezione dei dati, a seconda di quale sia la protezione maggiore.

3. Sicurezza Fisica e Controllo degli Ingressi (per come viene utilizzato di seguito, per "Struttura" si intende una sede fisica in cui il Fornitore ospita, elabora o altrimenti accedere a Materiale Kyndryl).

3.1. Il Fornitore manterrà un adeguato controllo degli ingressi, quali barriere, punti di ingresso controllati da badge, telecamere di sorveglianza e punti di accoglienza presidiati, per proteggere da ingressi non autorizzati alle Strutture.

3.2. Il Fornitore richiederà l'autorizzazione per consentire l'accesso alle Strutture ed alle aree controllate all'interno delle proprie Strutture, anche in caso di accesso temporaneo e limiterà l'accesso in base al ruolo professionale ed alle esigenze di business. Se il Fornitore concede un accesso temporaneo ad un visitatore, questo dovrà essere accompagnato all'interno della Struttura e in qualsiasi area controllata da un dipendente autorizzato del Fornitore.

3.3. Per limitare in modo appropriato l'ingresso alle aree controllate all'interno delle Strutture il Fornitore implementerà controlli di accesso fisici, inclusi controlli di accesso a più fattori aderenti alle Migliori Pratiche del Settore, registrerà tutti i tentativi di accesso e manterrà tali registri per almeno un anno.

3.4. Il Fornitore revocherà l'accesso alle Strutture e alle aree controllate all'interno delle Strutture (a) al momento dell'interruzione della collaborazione con un dipendente autorizzato del Fornitore o (b) dal momento in cui il dipendente autorizzato del Fornitore non avrà più un valido bisogno commerciale per l'accesso. Il Fornitore si atterrà alle procedure formali di separazione documentate che includono la rimozione tempestiva dalle liste di controllo accessi e la restituzione dei badge di accesso.

3.5. Il Fornitore adotterà precauzioni per proteggere l'infrastruttura fisica utilizzata per il supporto dei Servizi e dei Materiali da Consegnare da minacce ambientali, sia in caso di eventi naturali che causati dall'uomo quali, ad esempio, eccessiva temperatura dell'ambiente, incendi, inondazioni, umidità, furti e vandalismo.

4. Controllo Accessi, Interventi, Trasferimenti e Separazione

4.1. Il Fornitore manterrà un'architettura di sicurezza documentata delle reti che gestisce durante l'operatività dei Servizi, la fornitura dei Materiali da Consegnare e la Gestione della Tecnologia Kyndryl. Il Fornitore verificherà separatamente tale architettura di rete ed adotterà misure per prevenire

connessioni di rete non autorizzate a sistemi, applicazioni e dispositivi di rete, garantendo la conformità agli standard segmentazione sicura, isolamento e difesa. Il Fornitore non potrà utilizzare la tecnologia wireless per l'hosting e l'operatività di alcun Servizio Ospitato; il Fornitore potrà invece utilizzare la tecnologia di rete wireless per l'erogazione dei Servizi e dei Materiali da Consegnare e nella Gestione della Tecnologia Kyndryl, ma dovrà crittografare le comunicazioni e prevedere l'implementazione di un'autenticazione sicura su tali reti wireless.

4.2. Il Fornitore definirà e gestirà misure progettate allo scopo di separare logicamente i Materiali Kyndryl ed impedire che gli stessi siano esposti o accessibili a persone non autorizzate. Inoltre, il Fornitore manterrà un adeguato isolamento del proprio ambiente di produzione, non produzione e di altri ambienti e, nell'eventualità in cui del Materiale Kyndryl siano già presenti o vengano trasferiti in un ambiente non di produzione (ad esempio per riprodurre un errore), il Fornitore dovrà garantire che la sicurezza e la protezione della privacy nell'ambiente non di produzione siano uguali a quelle dell'ambiente di produzione.

4.3. Il Fornitore crittograferà i Materiali Kyndryl in transito e a riposo (a meno che il Fornitore non dimostri con ragionevole soddisfazione di Kyndryl che la crittografia del Materiale Kyndryl risulti tecnicamente impossibile). Il fornitore crittograferà anche tutti i supporti fisici, se presenti, quali ad esempio i supporti contenenti file di backup. Il Fornitore documenterà le procedure per la generazione, emissione, distribuzione, archiviazione, rotazione, revoca, ripristino, backup, distruzione, accesso e utilizzo di chiavi protette associate alla crittografia dei dati. Il Fornitore dovrà verificare che gli specifici metodi crittografici utilizzati per tale crittografia siano in linea con le Migliori Pratiche del Settore (come ad esempio NIST SP 800-131a).

4.4. Se il Fornitore richiede l'accesso al Materiale Kyndryl, il Fornitore vincolerà e limiterà tale accesso al livello minimo richiesto per l'erogazione e il supporto dei Servizi e dei Materiali da Consegnare. Il Fornitore dovrà richiedere che tale accesso, incluso l'accesso di amministratore a tutti i componenti sottostanti (ossia, accesso con privilegi), sia personale, basato sul ruolo e soggetto a convalida periodica da parte del personale del Fornitore autorizzato in base al principio della separazione dei compiti. Il Fornitore manterrà le misure per identificare e rimuovere account eccessivi e dormienti. Il Fornitore revocherà inoltre gli account con accesso privilegiato entro ventiquattro (24) ore dell'interruzione della collaborazione con il proprietario dell'account o dalla richiesta da parte di Kyndryl o di qualsiasi dipendente del Fornitore autorizzato, come ad esempio il manager del proprietario dell'account.

4.5. In conformità con le Migliori Pratiche del Settore, il Fornitore manterrà le misure tecniche applicando il timeout di sessioni inattive, il blocco degli account dopo molti tentativi di accesso sequenziali non riusciti, l'autenticazione complessa mediante password o passphrase e misure che richiedano un trasferimento protetto e la memorizzazione di tali password e passphrase. Inoltre, il Fornitore utilizzerà l'autenticazione a più fattori per tutti gli accessi privilegiati non basati su console a qualsiasi Materiale Kyndryl.

4.6. Il Fornitore monitorerà l'utilizzo dell'accesso con privilegi e manterrà le informazioni sulla sicurezza e le misure di gestione degli eventi progettate per 1) identificare accessi e attività non autorizzati, 2) agevolare una risposta tempestiva e appropriata a tali accessi e attività e 3) abilitare i controlli della conformità alle policy documentate del Fornitore da parte del Fornitore, di Kyndryl (ai sensi dei propri diritti di verifica contenuti nei presenti Termini e dei diritti di revisione contabile presenti nel Documento d'Ordine o nell'accordo base associato o in altro accordo correlato tra le parti) e di altri.

4.7. Il Fornitore conserverà i log, in conformità con le Migliori Pratiche del Settore, in cui registrerà tutti gli accessi o le attività amministrative, utente o di altro tipo in relazione ai sistemi utilizzati nell'erogazione di Servizi o Materiali da Consegnare e nella Gestione della Tecnologia Kyndryl (e su richiesta fornirà tali registri a Kyndryl). Il Fornitore manterrà le misure progettate per proteggere da accessi non autorizzati, modifica e distruzione accidentale o deliberata di tali log.

4.8. Il Fornitore manterrà le protezioni informatiche per i sistemi che possiede o gestisce, compresi i sistemi degli utenti finali, e che utilizza nella fornitura di Servizi o Materiali da Consegnare o nella Gestione della Tecnologia Kyndryl, con tali protezioni che includono: firewall endpoint, crittografia completa del disco, tecnologie di rilevamento e risposta degli endpoint basate su firma e non firma per affrontare malware e minacce persistenti avanzate, blocchi dello schermo basati sul tempo e soluzioni di gestione degli endpoint che applicano requisiti di configurazione della sicurezza e patch. Inoltre, il Fornitore

implementerà controlli tecnici e operativi che garantiranno che solo i sistemi di utenti finali noti e affidabili possano utilizzare le reti del Fornitore.

4.9. Coerentemente con le Migliori Pratiche del Settore, il Fornitore gestirà la protezione degli ambienti dei data center in cui sono presenti o viene elaborato il Materiali Kyndryl, con protezioni quali: rilevazione e prevenzione delle intrusioni e contromisure e mitigazione degli attacchi di tipo Denial of Service.

5. Controllo Integrità e Disponibilità del Servizio e dei Sistemi

5.1. Il Fornitore provvederà a: 1) effettuare almeno una volta l'anno la valutazione della sicurezza e dei rischi per la privacy, 2) eseguire i test di sicurezza e le valutazioni della vulnerabilità, inclusa la scansione automatica della sicurezza dei sistemi e delle applicazioni e l'hacking etico manuale, prima del rilascio in produzione e da quel momento una volta l'anno per i Servizi ed i Materiali da Consegnaree e annualmente per la Gestione della Tecnologia Kyndryl, 3) affidarsi a terze parti indipendenti qualificate per eseguire i test di penetrazione in conformità con le Migliori Pratiche del Settore, almeno una volta all'anno, 4) eseguire la verifica automatizzata della gestione e delle routine della conformità con i requisiti di configurazione della sicurezza di ciascun componente dei Servizi e dei Materiali da Consegnare ed in relazione alla propria Gestione della Tecnologia Kyndryl; e 5) correggere le vulnerabilità o le mancate conformità identificate con i relativi requisiti di configurazione della sicurezza in base al rischio, all'utilizzabilità e all'impatto associati. Il Fornitore adotterà ragionevoli misure per evitare l'interruzione dei Servizi durante l'esecuzione dei relativi test, valutazioni, scansioni ed esecuzione delle azioni correttive. Su richiesta di Kyndryl, il Fornitore fornirà a Kyndryl un riepilogo scritto delle proprie attività di test di penetrazione più recenti, che deve contenere almeno il nome delle offerte coperte dal test, il numero di sistemi o applicazioni inclusi nell'ambito del test, le date del test, la metodologia utilizzata per il test e un riepilogo di alto livello dei risultati.

5.2. Il Fornitore manterrà le politiche e le procedure progettate per gestire i rischi associati all'applicazione di modifiche ai Servizi, ai Materiali da Consegnare ed alla Gestione delle Tecniche Kyndryl. Prima di implementare tale modifica anche sui sistemi, sulle reti e sui componenti sottostanti interessati, il Fornitore documenterà, in una richiesta di modifica registrata: (a) una descrizione ed il motivo della modifica, (b) i dettagli di implementazione ed il relativo piano, (c) una dichiarazione dei rischi che riporti l'impatto di tale modifica sui Servizi e sui Materiali da Consegnare, per i clienti dei Servizi o sul Materiale Kyndryl, (d) il risultato previsto, (e) il piano di rollback, e (f) l'approvazione dei dipendenti autorizzati del Fornitore.

5.3. Il Fornitore terrà un inventario di tutte le risorse IT che utilizza per la gestione dei Servizi, per la fornitura dei Materiali da Consegnare e per la Gestione della Tecnologia Kyndryl. Il Fornitore monitorerà e gestirà costantemente l'integrità (compresa la capacità) e la disponibilità di tali asset IT, dei Servizi, dei Materiali da Consegnare e della Tecnologia Kyndryl, inclusi i componenti sottostanti di tali asset, Servizi, Materiali da Consegnare e Tecnologia Kyndryl.

5.4. Il Fornitore costruirà tutti i sistemi che utilizzerà nello sviluppo o nell'operatività dei Servizi ed i Materiali da Consegnaree e nella propria Gestione della Tecnologia Kyndryl, a partire dalle immagini predefinite di sicurezza di sistema o dalle linee di base di sicurezza definite in modo da soddisfare le Migliori Pratiche del Settore, quali ad esempio i benchmark del Center for Internet Security (CIS).

5.5. Senza limitazione delle obbligazioni del Fornitore o dei diritti di Kyndryl definiti nel Documento d'Ordine o nell'accordo base associatotra le parti, in merito alla continuità operativa, il Fornitore valuterà separatamente i requisiti di continuità operativa e IT e di disaster recovery di ciascuno dei Servizi e dei Materiali da Consegnare e di ciascun sistema IT utilizzato durante la Gestione della Tecnologia Kyndryl, in base alle linee guida documentate sulla gestione dei rischi. Il Fornitore dovrà assicurarsi che ciascuno dei Servizi, dei Materiali da Consegnare e dei sistemi IT sia dotato, nella misura garantita da tale valutazione del rischio, di piani di continuità operativa e IT e di disaster recovery definiti separatamente, documentati, manutenuti e convalidati ogni anno in conformità con le Migliori Pratiche del Settore. Il Fornitore dovrà garantire che tali piani siano progettati per assicurare dei tempi di ripristino specifici stabiliti nel seguente Articolo 5.6.

5.6. Gli **RPO** (recovery point objectives) e gli **RTO** (and recovery time objectives) specifici per ciascun Servizio Ospitato sono: 24 ore per gli RPO e 24 ore per gli RTO; tuttavia, nel caso in cui Kyndryl si impegni con un Cliente al rispetto di un RPO o di un RTO più breve, il Fornitore, previa comunicazione

per iscritto di Kyndryl, si atterrà prontamente al rispetto degli RPO o RTO comunicati da Kyndryl (una e-mail costituisce una scrittura). Per quanto riguarda tutti gli altri Servizi erogati dal Fornitore a Kyndryl, il Fornitore dovrà garantire che i piani di continuità aziendale e di disaster recovery siano progettati per fornire RPO e RTO che consentano al Fornitore di rispettare le proprie obbligazioni nei confronti di Kyndryl ai sensi del Documento d'Ordine e dell'accordo base tra le parti ed i presenti Termini, incluse le obbligazioni a fornire tempestivamente test, supporto e manutenzione.

5.7. Il Fornitore manterrà le misure progettate per valutare, testare e applicare le patch degli avvisi di sicurezza per i Servizi e per i Materiali da Consegnare e per i sistemi, reti, applicazioni e componenti sottostanti associati inclusi nell'ambito di tali Servizi e Materiali da Consegnare così come per i sistemi, reti, applicazioni e componenti sottostanti utilizzati per la Gestione della Tecnologia Kyndryl. Dopo aver stabilito che una patch degli avvisi di sicurezza è applicabile e appropriata, il Fornitore implementerà la patch in base alla severità e alle linee guida documentate sulla valutazione del rischio. L'implementazione da parte del Fornitore delle patch degli avvisi di sicurezza sarà soggetta alla policy di gestione delle modifiche del Fornitore.

5.8. Se Kyndryl ha fondati motivi per ritenere che l'hardware o il software forniti dal Fornitore possano contenere elementi intrusivi, quali spyware, malware o codice dannoso, il Fornitore collaborerà tempestivamente con Kyndryl per indagare e risolvere le preoccupazioni di Kyndryl.

6. Provisioning dei Servizi

6.1 Il Fornitore supporterà metodi comuni di autenticazione federata per gli account dell'utente Kyndryl o del Cliente, con il Fornitore che si atterrà alle Migliori Pratiche del Settore per l'autenticazione di tali account dell'utente Kyndryl o del Cliente (con ad esempio il Single Sign-On (SSO) multi-fattore gestito centralmente da Kyndryl, con OpenID Connect (OIDC) o con Security Assertion Markup Language).

7. Subfornitori. Senza limitazione delle obbligazioni del Fornitore o dei diritti di Kyndryl definiti nel Documento d'Ordine o nell'accordo base associato tra le parti, in merito alla conservazione dei subappaltatori, il Fornitore garantirà che qualsiasi subappaltatore che esegua lavori per il Fornitore abbia istituito controlli di governance per conformarsi ai requisiti e alle obbligazioni imposte al Fornitore dai presenti Termini.

8. Supporti Fisici. Il Fornitore bonificherà in modo sicuro i supporti fisici destinati al riutilizzo prima di tale riutilizzo e distruggerà i supporti fisici che non devono essere riutilizzati, in conformità con le Migliori Pratiche del Settore in materia di bonifica dei supporti.

Articolo IX, Certificazioni e Report dei Servizi Ospitati

Questo Articolo si applica se il Fornitore offre un Servizio Ospitato a Kyndryl.

1.1 Il Fornitore dovrà ottenere le seguenti certificazioni o report entro i tempi indicati di seguito:

Certificazioni / Report	**Intervallo di tempo**
In relazione ai Servizi Ospitati dal Fornitore: Certificazione di conformità con ISO 27001, Information Technology, Tecniche di sicurezza, Sistemi di gestione della sicurezza delle informazioni, con tali certificazioni basate sulla valutazione di un revisore indipendente affidabile **Oppure** SOC 2 Type 2: Un report di un revisore indipendente attendibile che dimostri l'avvenuta revisione dei sistemi, dei controlli e delle operazioni del Fornitore secondo gli standard SOC 2 Type 2 (includendo, come minimo, sicurezza, riservatezza e disponibilità).	Il Fornitore otterrà la certificazione ISO 27001 entro 120 giorni dalla data di entrata in vigore del presente Documento d'Ordine* o dalla Data di Assunzione**, quindi da quel momento provvederà a rinnovare la certificazione ogni 12 mesi in base alla valutazione di un revisore indipendente affidabile (ogni rinnovo dovrà essere effettuato nel rispetto della versione più aggiornata della norma) Il Fornitore otterrà il report SOC2 Type 2 entro 240 giorni dalla data di entrata in vigore del presente Documento d'Ordine* o dalla Data di Assunzione** e quindi garantirà il rinnovo del report da parte di un revisore indipendente attendibile che dimostri l'avvenuta revisione dei sistemi, dei controlli e delle operazioni del Fornitore secondo gli standard SOC 2 Type 2 (includendo, come minimo, sicurezza, riservatezza e disponibilità) ogni 12 mesi a partire da tale data * Se, a partire da tale data di entrata in vigore, il Fornitore fornisce un Servizio Ospitato ** La data in cui il Fornitore assume l'obbligazione di fornire un Servizio Ospitato

1.2 Dopo richiesta per iscritto del Fornitore e relativa approvazione per iscritto di Kyndryl, il Fornitore potrà ottenere una certificazione o un report sostanzialmente equivalente a quelli indicati in precedenza, con la consapevolezza che gli intervalli di tempo stabiliti nella tabella precedente si applicheranno invariati alla certificazione o report sostanzialmente equivalente.

1.3 Il Fornitore provvederà a: i) fornire tempestivamente a Kyndryl, su richiesta, una copia di ciascuna certificazione e report che il Fornitore è tenuto ad ottenere e ii) risolvere prontamente eventuali carenze del controllo interno rilevate durante le revisioni SOC 2 o le revisioni sostanzialmente equivalenti (se approvate da Kyndryl).

Articolo X, Cooperazione, Verifica e Rimedio

Questo Articolo si applica se il Fornitore offre un Servizio o dei Materiali da Consegnare a Kyndryl.

1. Cooperazione dei Fornitore

1.1. Se Kyndryl ha motivo credere che alcuni Servizi o Materiali da Consegnare possano aver contribuito, stiano contribuendo o contribuiranno a qualsiasi problema di sicurezza informatica, il Fornitore collaborerà ragionevolmente a rispondere a qualsiasi domanda di Kyndryl relativa a tale preoccupazione, anche rispondendo tempestivamente e pienamente alle richieste di informazioni, attraverso documenti, altri registri, colloqui con il Personale del Fornitore, o simili.

1.2. Le parti concordano a: (a) fornire su richiesta reciproca tali ulteriori informazioni, (b) creare e consegnare reciprocamente tali altri documenti e (c) compiere tali altri atti e cose, tutto ciò che l'altra parte possa ragionevolmente richiedere allo scopo di realizzare l'intento dei presenti Termini e dei documenti a cui si fa riferimento nei presenti Termini. Ad esempio, se Kyndryl lo richiede, il Fornitore fornirà tempestivamente i termini riguardanti privacy e sicurezza dei propri contratti scritti con i Subresponsabili e con i subappaltatori, incluso, laddove il Fornitore abbia il diritto di farlo, concedendo l'accesso ai contratti stessi.

1.3. Se Kyndryl lo richiede, il Fornitore fornirà tempestivamente informazioni sui paesi in cui i propri Materiali da Consegnare e componenti sono stati prodotti, sviluppati o altrimenti acquistati.

2. Verifica (per come viene utilizzato di seguito, per "Struttura" si intende una sede fisica in cui il Fornitore ospita, elabora o altrimenti accedere al Materiale Kyndryl)

2.1. Il fornitore manterrà un registro verificabile che dimostri la conformità ai presenti Termini.

2.2. Kyndryl, da sola o con l'ausilio di un revisore esterno, potrà, con preavviso scritto di 30 giorni al Fornitore, verificare il rispetto da parte del Fornitore dei presenti Termini, anche accedendo a qualsiasi Struttura per tale scopo, sebbene Kyndryl non accederà ad alcun data center in cui il Fornitore Tratta Dati Kyndryl a meno che non abbia in buona fede motivo di ritenere che ciò fornirebbe informazioni pertinenti. Il Fornitore collaborerà nelle verifiche di Kyndryl anche rispondendo tempestivamente e pienamente alle richieste di informazioni, attraverso documenti, altri registri, colloqui con il Personale del Fornitore, o simili. Il Fornitore può fornire la prova dell'adesione a un codice di condotta approvato o una certificazione del settore o fornire in altro modo informazioni per dimostrare la conformità ai presenti Termini, a titolo oneroso da parte di Kyndryl.

2.3. Le verifiche non avverranno con una cadenza inferiore ai 12 mesi, a meno che: (a) Kyndryl non stia convalidando i rimedi messi in atto dal Fornitore rispetto alle preoccupazioni risultanti da una verifica precedente e più recente di 12 mesi o (b) sia stata rilevata una Violazione della Sicurezza e Kyndryl desideri verificare il rispetto delle obbligazioni in relazione a tale violazione. In entrambi i casi, Kyndryl fornirà lo stesso preavviso scritto di 30 Giorni come specificato nel precedente Articolo 2.2, ma l'urgenza di far fronte a una Violazione della Sicurezza potrà richiedere a Kyndryl di effettuare una verifica con preavviso scritto inferiore a 30 giorni.

2.4. Un organismo regolatore o un Altro Titolare del Trattamento dei Dati Personali potrà esercitare gli stessi diritti di Kyndryl, riportati negli Artt. 2.2 e 2.3, con la consapevolezza che un organismo regolatore potrà esercitare tutti i diritti aggiuntivi di cui dispone ai sensi della legge.

2.5. Se Kyndryl ha basi ragionevoli per concludere che il Fornitore non è conforme con i presenti Termini (indipendentemente dal fatto che tali basi derivino da una verifica ai sensi dei presenti Termini o altro), il Fornitore rimedierà prontamente tale non conformità.

3. Programma Anti-Contraffazione

3.1. Se i Materiali da Consegnare offerti dal Fornitore includono componenti elettronici (ad esempio, unità disco fisso, unità solid-state, memoria, CPU, dispositivi logici o cavi), il Fornitore manterrà e seguirà un programma documentato di prevenzione della contraffazione per impedire, in primo luogo, al Fornitore di consegnare componenti contraffatti a Kyndryl e, secondariamente, rilevare e rimediare

tempestivamente ad ogni caso in cui il Fornitore consegni erroneamente componenti contraffatti a Kyndryl. Il Fornitore imporrà lo stesso obbligazione di mantenere e seguire un programma documentato di prevenzione della contraffazione a tutti i propri fornitori che consegnano componenti elettronici che sono inclusi nei Materiali da Consegnare del Fornitore a Kyndryl.

4. Remedi

4.1. Se il Fornitore non adempie a uno qualsiasi delle proprie obbligazioni ai sensi dei presenti Termini e tale mancanza provoca una Violazione della Sicurezza, allora il Fornitore deve porre rimedio tale inadempimento delle proprie prestazioni e agli effetti dannosi della Violazione della Sicurezza. Tali prestazioni e rimedi saranno effettuati secondo la ragionevole indicazioni e pianificazione di Kyndryl. Tuttavia, qualora la Violazione della Sicurezza, derivi dall'erogazione da parte del Fornitore di un Servizio Ospitato multi-tenant e, di conseguenza, tale violazione abbia un impatto su molti clienti del Fornitore, tra cui Kyndryl, il Fornitore dovrà, data la natura della Violazione della Sicurezza, porre rimedio a tale inadempimento delle proprie prestazioni e agli effetti dannosi della Violazione della Sicurezza, tenendo al contempo in debita considerazione qualsiasi input Kyndryl su tali correzioni e rimedi.

4.2. Kyndryl avrà il diritto di partecipare alla riparazione di qualsiasi Violazione della Sicurezza di cui all'Articolo 4.1, come ritiene opportuno o necessario, e il Fornitore sarà responsabile per i costi e le spese derivanti dalla correzione delle proprie prestazioni e per i costi e le spese sostenute dalle parti per le azioni di rimedio in relazione a tali Violazioni della Sicurezza.

4.3. A titolo di esempio, i costi e le spese di qualsiasi rimedio associato a una Violazione della Sicurezza potrebbero includere quelli per il rilevamento e l'indagine di una Violazione della Sicurezza, la determinazione delle responsabilità ai sensi delle leggi e dei regolamenti applicabili, la esecuzione di notifiche della violazione, la creazione e la manutenzione di call center, il monitoraggio del credito ed i servizi di ripristino del credito, il ricaricamento dei dati, la correzione dei difetti del prodotto (anche attraverso il Codice Sorgente o altre attività di sviluppo), il trattenere terze parti per fornire assistenza su quanto sopra o altre attività pertinenti e altri costi e spese necessari per rimediare agli effetti dannosi della Violazione della Sicurezza. Per chiarezza, i costi e le spese di rimedio non includeranno perdite di profitto, di opportunità commerciali, di valore, di fatturato, di avviamento o di previsti risparmi.