Artykuł I. Biznesowe Informacje Kontaktowe

Niniejszy Artykuł ma zastosowanie w przypadku, gdy jedna ze Stron, tj. Dostawca lub Kyndryl, Przetwarza Biznesowe Informacje Kontaktowe drugiej Strony.

1.1 Każda ze Stron, tj. Kyndryl i Dostawca, może Przetwarzać Biznesowe Informacje Kontaktowe drugiej Strony, jeśli prowadzi działalność biznesową w związku ze świadczeniem przez Dostawcę Usług i udostępnianiem przez niego Produktów Dostarczanych.

1.2 W związku z tym Strony mają następujące obowiązki:

(a) żadna ze Stron nie będzie używać ani ujawniać Biznesowych Informacji Kontaktowych drugiej Strony w jakimkolwiek innym celu (dla ścisłości ustala się, że żadna ze Stron nie będzie Sprzedawać Biznesowych Informacji Kontaktowych drugiej Strony, ani też ich używać lub ujawniać w jakimkolwiek celu marketingowym bez uprzedniej pisemnej zgody drugiej Strony, a jeśli jest to wymagane, również Podmiotów Danych, których te dane dotyczą), oraz

(b) każda ze Stron usunie, zmodyfikuje, skoryguje, zwróci, przekaże informacje na temat Przetwarzania, ograniczy Przetwarzanie oraz podejmie wszelkie inne uzasadnione i wymagane działania w odniesieniu do Biznesowych Informacji Kontaktowych drugiej Strony, bezzwłocznie po otrzymaniu od takiej Strony pisemnej prośby, zawsze gdy wystąpi nieuprawnione wykorzystanie danych osobowych, a Strona chce przerwać przetwarzanie i naprawić szkody.

1.3 Strony nie nawiązują relacji współadministratorów (tj. takiej, w której każda ze Stron staje się współadministratorem Biznesowych Informacji Kontaktowych drugiej Strony), a żadne z postanowień Dokumentu Transakcyjnego nie będzie interpretowane jako intencja nawiązania takiej relacji.

1.4 Więcej informacji na temat Przetwarzania przez Kyndryl Biznesowych Informacji Kontaktowych jest zawarte w Oświadczeniu Kyndryl o Ochronie Prywatności, dostępnym pod adresem https://www.kyndryl.com/us/en/privacy.

1.5 Strony zaimplementowały i będą utrzymywać środki techniczne i organizacyjne w zakresie bezpieczeństwa, aby zabezpieczyć Biznesowe Informacje Kontaktowe drugiej Strony przed utratą, zniszczeniem, zmianą, ujawnieniem przypadkowym lub ujawnieniem bez zezwolenia, dostępem przypadkowym lub dostępem bez zezwolenia oraz wszelkimi niezgodnymi z prawem formami Przetwarzania.

1.6 Dostawca niezwłocznie (i w każdym przypadku przed upływem 48 godzin) powiadomi firmę Kyndryl o wszelkich wykrytych naruszeniach bezpieczeństwa, w związku z Biznesowymi Informacjami Kontaktowymi firmy Kyndryl. Dostawca jest zobowiązany przesłać takie powiadomienie na adres cyber.incidents@kyndryl.com . Dostawca dostarczy firmie Kyndryl żądane (w uzasadnionym zakresie) informacje o naruszeniu bezpieczeństwa, oraz o statusie działań naprawczych i działań w zakresie przywracania, podjętych przez Dostawcę. Informacje takie mogą na przykład obejmować dzienniki pokazujące dostęp do Urządzeń, systemów lub aplikacji uzyskiwany przez użytkowników uprzywilejowanych, użytkowników na prawach administratora i innych użytkowników, a także obrazy Urządzeń, systemów, aplikacji i innych podobnych elementów na potrzeby badania incydentów w zakresie, który jest odpowiedni do naruszenia lub podjętych przez Dostawcę czynności naprawczych oraz działań mających na celu odzyskanie danych.

1.7 Jeśli Dostawca Przetwarza tylko Biznesowe Informacje Kontaktowe Kyndryl i nie ma dostępu do żadnych innych danych lub materiałów, ani też do Systemu Korporacyjnego Kyndryl, to wówczas do takiego

Przetwarzania ma zastosowanie wyłącznie niniejszy Artykuł oraz Artykuł X (Współpraca, weryfikacja i czynności naprawcze).

Artykuł II. Środki techniczne i organizacyjne. Bezpieczeństwo danych

Niniejszy Artykuł ma zastosowanie w przypadku, gdy Dostawca Przetwarza Dane Kyndryl inne niż Biznesowe Informacje Kontaktowe Kyndryl. Podczas świadczenia wszelkich Usług i udostępniania Produktów Dostarczanych Dostawca będzie przestrzegać wymagań określonych w niniejszym Artykule i w ten sposób chronić Dane Kyndryl przed utratą, zniszczeniem, zmianą, ujawnieniem przypadkowym lub ujawnieniem bez zezwolenia, dostępem przypadkowym lub dostępem bez zezwolenia oraz wszelkimi niezgodnymi z prawem formami Przetwarzania. Wymagania określone w niniejszym Artykule obowiązują w odniesieniu do wszelkich aplikacji, platform i infrastruktur informatycznych, które Dostawca wykorzystuje w celu udostępniania Produktów Dostarczanych i świadczenia Usług, w tym wszelkich środowisk programowania, testowania, udostępniania, wsparcia i eksploatacji oraz centrów przetwarzania danych.

1. Wykorzystanie danych

1.1 Dostawca nie może dodawać do Danych Kyndryl ani włączać w nie żadnych innych informacji lub danych, w tym Danych Osobowych, bez wcześniejszej pisemnej zgody Kyndryl. Dostawca nie może też używać Danych Kyndryl w żadnej formie, również zbiorczej, w jakimkolwiek celu innym niż świadczenie Usług i udostępnianie Produktów Dostarczanych (przykładowo, Dostawcy nie wolno używać ani ponownie wykorzystywać Danych Kyndryl do oceny skuteczności lub jako sposobu na poprawę produktów i usług oferowanych przez Dostawcę, na potrzeby prac badawczo-rozwojowych przy tworzeniu nowych produktów lub usług, ani do generowania raportów dotyczących produktów i usług Dostawcy). O ile nie jest to wyraźnie dozwolone w Dokumencie Transakcyjnym, Dostawca nie może Sprzedawać Danych Kyndryl.

1.2 Dostawca nie będzie włączać w swoje Usługi lub Produkty Dostarczane technologii monitorowania aktywności na stronach WWW (takich jak HTML5, pamięć lokalna, znaczniki lub tokeny osób trzecich czy sygnalizatory WWW), o ile nie jest to wyraźnie dozwolone w Dokumencie Transakcyjnym.

2. Wnioski osób trzecich i zachowanie poufności

2.1 Dostawca nie będzie ujawniać Danych Kyndryl jakimkolwiek osobom trzecim bez uprzedniego pisemnego zezwolenia Kyndryl. Jeśli rząd, w tym jakikolwiek organ regulacyjny, zażąda dostępu do Danych Kyndryl (np. jeśli rząd Stanów Zjednoczonych wyda nakaz podyktowany względami bezpieczeństwa narodowego, który wymaga od Dostawcy uzyskania Danych Kyndryl), lub jeśli ujawnienie Danych Kyndryl jest wymagane przez prawo na innych podstawach, to Dostawca powiadomi Kyndryl na piśmie o takim żądaniu lub wymaganiu oraz zapewni Kyndryl rozsądną możliwość zakwestionowania konieczności ujawnienia Danych Kyndryl (jeśli istnieje zakaz, który uniemożliwia Dostawcy przekazanie Kyndryl takiego powiadomienia, to Dostawca podejmie działania, które uzna za odpowiednie, w celu uzyskania zwolnienia z tego zakazu i niedopuszczenia do ujawnienia Danych Kyndryl na drodze sądowej lub w inny sposób).

2.2 Dostawca zapewnia Kyndryl, że: (a) dostęp do Danych Kyndryl będą mieć tylko ci pracownicy Dostawcy, którzy potrzebują go w celu świadczenia Usług lub udostępniania Produktów Dostarczanych, przy czym dostęp ten będzie ograniczony do zakresu niezbędnego w tym celu; (b) zobowiązał swoich pracowników do zachowania poufności, tak aby używali i ujawniali Dane Kyndryl tylko zgodnie z niniejszymi Warunkami.

3. **Zwrot lub usuwanie danych Kyndryl**

3.1 Dostawca, według uznania Kyndryl, po wygaśnięciu lub rozwiązaniu Dokumentu Transakcyjnego, lub wcześniej na żądanie Kyndryl, usunie lub zwróci Dane Kyndryl. Jeśli Kyndryl wymaga usunięcia Danych Kyndryl, wówczas Dostawca usunie je zgodnie ze Sprawdzonymi Procedurami Branżowymi w taki sposób, że będą nieczytelne i niemożliwe do ponownego złożenia w całość lub odtworzenia, oraz przedstawi Kyndryl poświadczenie takiego usunięcia. Jeśli Kyndryl zażąda zwrotu Danych Kyndryl, Dostawca zwróci je w rozsądnym terminie określonym przez Kyndryl, zgodnie z uzasadnionymi instrukcjami Kyndryl przekazanymi na piśmie.

Artykuł III. Ochrona prywatności

Niniejszy Artykuł ma zastosowanie w przypadku, gdy Dostawca Przetwarza Dane Osobowe Kyndryl.

1. Przetwarzanie

1.1 Kyndryl mianuje Dostawcę Administratorem, który będzie Przetwarzać Dane Osobowe Kyndryl wyłącznie na potrzeby udostępniania Produktów Dostarczanych i świadczenia Usług zgodnie z instrukcjami Kyndryl, w tym instrukcjami zawartymi w niniejszych Warunkach, Dokumencie Transakcyjnym oraz powiązanej umowie podstawowej zawartej pomiędzy Stronami. Jeśli Dostawca nie będzie się stosować do tych instrukcji, Kyndryl może wypowiedzieć odpowiednią część Usług, powiadamiając o tym Dostawcę na piśmie. Jeśli Dostawca uzna, że konkretna instrukcja narusza regulacje dotyczące ochrony danych osobowych, poinformuje o tym Kyndryl niezwłocznie, nie później niż w terminie wymaganym przez prawo. Jeżeli Dostawca zaniecha wykonania dowolnego ze swoich obowiązków wynikających z niniejszych Warunków, a takie zaniechanie spowoduje nieuprawnione użycie Danych Osobowych lub, ogólnie w przypadku jakiegokolwiek nieuprawnionego wykorzystania Danych Osobowych, firmie Kyndryl przysługuje prawo do przerwania przetwarzania oraz naprawienia zaniechania i wyeliminowania szkodliwych efektów nieuprawnionego użycia, przy czym takie działanie i naprawę Kyndryl wykona w ustalony przez siebie sposób i w wybranym terminie.

1.2 Dostawca będzie przestrzegać wszelkich regulacji dotyczących ochrony danych osobowych, które mają zastosowanie do Usług i Produktów Dostarczanych.

1.3 Załącznik szczegółowy do Dokumentu Transakcyjnego lub sam Dokument Transakcyjny określa w odniesieniu do Danych Kyndryl:

(a) kategorie Podmiotów Danych;
(b) rodzaje Danych Osobowych Kyndryl;
(c) czynności dotyczące danych i Przetwarzania;
(d) czas trwania i częstotliwość Przetwarzania;
(e) listę Podwykonawców Podmiotu Przetwarzającego.

2. Środki techniczne i organizacyjne

2.1 Dostawca wdroży i będzie utrzymywać środki techniczne i organizacyjne określone w Artykule II (Środki techniczne i organizacyjne. Bezpieczeństwo danych) i Artykule VIII (Środki techniczne i organizacyjne. Bezpieczeństwo ogólne) w celu zapewnienia poziomu bezpieczeństwa dostosowanego do ryzyka, jakie stwarzają jego Usługi i Produkty Dostarczane. Dostawca potwierdza i przyjmuje do wiadomości ograniczenia zawarte w Artykule II, niniejszym Artykule III i Artykule VIII oraz zobowiązuje się do ich przestrzegania.

3. Prawa i wnioski Podmiotów Danych

3.1 Dostawca będzie bez zbędnej zwłoki informować Kyndryl (w terminie umożliwiającym Kyndryl i Innym Administratorom wypełnienie zobowiązań prawnych) o wnioskach odnoszących się do Danych Osobowych Kyndryl, otrzymywanych od Podmiotów Danych korzystających ze swoich praw (np. prawa do sprostowania, usunięcia i zablokowania danych). Dostawca może także niezwłocznie skierować Podmiot Danych zgłaszający taki wniosek do Kyndryl. Dostawca nie będzie odpowiadać na żadne wnioski Podmiotów Danych, jeśli nie jest do tego zobowiązany na mocy przepisów lub jeśli Kyndryl nie poleci mu tego na piśmie.

3.2 Jeśli Kyndryl jest zobowiązany do udostępnienia informacji dotyczących Danych Osobowych Kyndryl Innym Administratorom lub innym osobom trzecim (np. Podmiotom Danych lub organom regulacyjnym), to Dostawca pomoże Kyndryl, dostarczając mu wszelkie informacje i podejmując uzasadnione działania wymagane przez Kyndryl, w czasie umożliwiającym Kyndryl terminowe udzielenie odpowiedzi takim Innym Administratorom lub innym osobom trzecim.

4. Podwykonawcy Podmiotu Przetwarzającego

4.1 Dostawca z wyprzedzeniem dostarczy Kyndryl pisemne powiadomienie o dodaniu nowego Podwykonawcy Podmiotu Przetwarzającego lub rozszerzeniu zakresu Przetwarzania przez dotychczasowego Podwykonawcę Podmiotu Przetwarzającego. Takie pisemne powiadomienie będzie zawierać nazwę (nazwisko) Podwykonawcy Podmiotu Przetwarzającego oraz opis nowego lub rozszerzonego zakresu Przetwarzania. Kyndryl może w każdej chwili na uzasadnionych podstawach sprzeciwić się dodaniu takiego nowego Podwykonawcy Podmiotu Przetwarzającego lub rozszerzeniu zakresu Przetwarzania. W takim przypadku obie Strony podejmą współpracę w dobrej wierze w celu rozpatrzenia takiego sprzeciwu ze strony Kyndryl. Z zastrzeżeniem prawa Kyndryl do takiego sprzeciwu, Dostawca może zlecić dodanie nowego Podwykonawcy Podmiotu Przetwarzającego lub rozszerzenie Przetwarzania przez dotychczasowego Podwykonawcę Podmiotu Przetwarzającego, jeśli Kyndryl nie wniósł sprzeciwu w ciągu 30 dni od daty pisemnego powiadomienia otrzymanego od Dostawcy.

4.2 Przed rozpoczęciem Przetwarzania Danych Kyndryl przez każdego zatwierdzonego Podwykonawcę Podmiotu Przetwarzającego Dostawca zobowiąże go do przyjęcia zobowiązań dotyczących ochrony danych, bezpieczeństwa i certyfikacji, które zostały określone w niniejszych Warunkach. Dostawca ponosi pełną odpowiedzialność wobec Kyndryl za realizację zobowiązań każdego Podwykonawcy Podmiotu Przetwarzającego.

5. Transgraniczne przetwarzanie danych

Używane poniżej terminy mają następujące znaczenie:

Kraj Zapewniający Odpowiedni Poziom Ochrony oznacza kraj, który zapewnia odpowiedni poziom ochrony danych w odniesieniu do stosownego przekazywania zgodnie z obowiązującymi regulacjami dotyczącymi ochrony danych osobowych lub decyzjami organów regulacyjnych.

Importer Danych oznacza Podmiot Przetwarzający lub Podwykonawcę Podmiotu Przetwarzającego, który nie ma siedziby w Kraju Zapewniającym Odpowiedni Poziom Ochrony.

Standardowe Klauzule Umowne UE („SKU UE") oznaczają Standardowe Klauzule Umowne UE (Decyzja Komisji 2021/914) z zastosowanymi klauzulami opcjonalnymi, z wyłączeniem opcji 1 Klauzuli 9(a) i opcji 2 Klauzuli 17, zgodnie z oficjalną publikacją pod adresem https://commission.europa.eu/publications/standard-contractual-clauses-international-transfers_en

Serbskie Standardowe Klauzule Umowne („Serbskie SKU") oznaczają serbskie Standardowe Klauzule Umowne przyjęte przez „Serbskiego Komisarza ds. Informacji o Znaczeniu Publicznym i Ochrony Danych Osobowych" oraz opublikowane pod adresem https://www.poverenik.rs/images/stories/dokumentacija-nova/podzakonski-akti/Klauzulelat.docx.

Standardowe Klauzule Umowne („**SKU**") oznaczają klauzule umowne wymagane przez obowiązujące regulacje dotyczące ochrony danych osobowych w odniesieniu do przesyłania Danych Osobowych do Podmiotów Przetwarzających, które to podmioty nie mają siedziby w Krajach Zapewniających Odpowiedni Poziom Ochrony Danych.

Dodatek do Standardowych Klauzul Umownych Komisji UE dotyczący Międzynarodowego Transferu Danych w Wielkiej Brytanii („Dodatek Brytyjski") oznacza Dodatek do Standardowych Klauzul Umownych Komisji UE dotyczący międzynarodowego transferu danych w Wielkiej Brytanii oficjalnie opublikowany na stronie https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-Transfer-agreement-and-guidance/.

Szwajcarski Dodatek do Standardowych Klauzul Umownych Komisji UE („Szwajcarski Dodatek")

oznacza klauzule umowne dla Standardowych Klauzul Umownych Komisji UE, które są stosowane zgodnie z orzeczeniem Szwajcarskiego Urzędu Ochrony Danych (**„FDPIC”**) oraz zgodnie ze Szwajcarską Federalną Ustawą o Ochronie Danych (**„FADP”**).

5.1 Bez wcześniejszej pisemnej zgody Kyndryl Dostawca nie będzie przekazywać ani ujawniać za granicą (w tym przez dostęp zdalny) żadnych Danych Osobowych Kyndryl. Jeśli Kyndryl udzieli takiej zgody, Strony podejmą współpracę w celu zapewnienia zgodności z obowiązującymi regulacjami dotyczącymi ochrony danych osobowych. Jeśli regulacje te wymagają stosowania Standardowych Klauzul Umownych, Dostawca na żądanie Kyndryl niezwłocznie podpisze takie klauzule.

5.2 W odniesieniu do Standardowych Klauzul Umownych UE:

(a) Jeśli Dostawca nie ma siedziby w Kraju Zapewniającym Odpowiedni Poziom Ochrony, to: Dostawca niniejszym zawiera z Kyndryl Standardowe Klauzule Umowne UE jako Importer Danych oraz zawrze z każdym zatwierdzonym Podwykonawcą Podmiotu Przetwarzającego pisemną umowę zgodnie z Klauzulą 9 Standardowych Klauzul Umownych UE i na żądanie dostarczy Kyndryl kopie takich umów.

(i) Moduł 1 Standardowych Klauzul Umownych UE nie ma zastosowania, chyba że Strony uzgodniły inaczej na piśmie.

(ii) Moduł 2 Standardowych Klauzul Umownych UE ma zastosowanie w przypadku, gdy Kyndryl jest Administratorem, a Moduł 3 ma zastosowanie w przypadku, gdy Kyndryl jest Podmiotem Przetwarzającym. Zgodnie z Klauzulą 13 Standardowych Klauzul Umownych UE, w przypadku zastosowania Modułu 2 lub 3, Strony zgadzają się, że (1) Standardowe Klauzule Umowne UE będą podlegać prawu państwa członkowskiego UE, w którym znajduje się właściwy organ nadzorczy, oraz (2) wszelkie spory wynikające ze Standardowych Klauzul Umownych UE będą rozstrzygane przez sądy państwa członkowskiego UE, w którym znajduje się właściwy organ nadzorczy. Jeśli prawo, o którym mowa w punkcie (1), nie dopuszcza praw beneficjentów będących osobami trzecimi, wówczas Standardowe Klauzule Umowne UE podlegają prawu Niderlandów, a wszelkie spory wynikające ze Standardowych Klauzul Umownych UE zgodnie z punktem (2) będą rozstrzygane przez sąd w Amsterdamie w Niderlandach.

(b) Jeżeli siedziby obu Stron, tj. Dostawcy i Kyndryl, znajdują się w Kraju Zapewniającym Odpowiedni Poziom Ochrony, wówczas Dostawca występuje w charakterze Eksportera Danych i zawiera Standardowe Klauzule Umowne UE z każdym zatwierdzonym Podwykonawcą Podmiotu Przetwarzającego mającym siedzibę w Kraju Niezapewniającym Odpowiedniego Poziomu Ochrony. Dostawca przeprowadzi wymaganą Ocenę Wpływu Transferu i bez zbędnej zwłoki powiadomi Kyndryl o (1) jakiejkolwiek konieczności podjęcia dodatkowych środków oraz o (2) już zastosowanych środkach. Na żądanie Dostawca dostarczy Kyndryl wyniki Oceny Wpływu Transferu oraz wszelkie informacje niezbędne do zrozumienia i ocenienia tych wyników. Jeżeli Kyndryl nie zgadza się z wynikami Oceny Wpływu Transferu przeprowadzonej przez Dostawcę lub zastosowanymi środkami dodatkowymi, Kyndryl i Dostawca wspólnie postarają się znaleźć wykonalne rozwiązanie. Kyndryl zachowuje prawo do zawieszenia lub zakończenia usług Dostawcy bez przyznawania wynagrodzenia. Dla uniknięcia wątpliwości, nie zwalnia to Podwykonawców Podmiotu Przetwarzającego ze strony Dostawcy z obowiązku podpisania Standardowych Klauzul Umownych UE z Kyndryl lub jego Klientami, jak określono w paragrafie 5.2 (d) poniżej.

(c) Jeśli Dostawca ma siedzibę w Europejskim Obszarze Gospodarczym, a Kyndryl jest Administratorem niepodlegającym Ogólnemu rozporządzeniu o ochronie danych 2016/679, to ma zastosowanie Moduł 4 Standardowych Klauzul Umownych UE, a Dostawca niniejszym zawiera z Kyndryl Standardowe Klauzule Umowne UE jako eksporter danych. W przypadku zastosowania Modułu 4 Standardowych Klauzul Umownych UE Strony zgadzają się, że Standardowe Klauzule Umowne UE podlegają prawu Niderlandów, a wszelkie spory

wynikające ze Standardowych Klauzul Umownych UE będą rozstrzygane przez sąd w Amsterdamie w Niderlandach.

(d) Jeśli Inni Administratorzy, tacy jak Klienci lub przedsiębiorstwa afiliowane, zwrócą się z wnioskiem o przyjęcie Standardowych Klauzul Umownych UE zgodnie z „klauzulą dokującą" zawartą w Klauzuli 7, Dostawca niniejszym wyraża zgodę na każdy taki wniosek.

(e) Środki techniczne i organizacyjne wymagane do wypełnienia postanowień Załącznika II do Standardowych Klauzul Umownych można znaleźć w niniejszych Warunkach, samym Dokumencie Transakcyjnym oraz powiązanej z nim umowie podstawowej zawartej pomiędzy Stronami.

(f) W przypadku sprzeczności pomiędzy Standardowymi Klauzulami Umownymi UE a niniejszymi Warunkami znaczenie rozstrzygające będą mieć Standardowe Klauzule Umowne UE.

5.3 Dotyczy Dodatku(-ów) Brytyjskiego(-ich):

(a) Jeśli Dostawca nie ma siedziby w Kraju Zapewniającym Odpowiedni Poziom Ochrony: (i) Dostawca niniejszym zawiera z Kyndryl jako Importerem Dodatek(-ki) Brytyjski(e) w celu uzupełnienia Standardowych Klauzul Umownych UE określonych powyżej (w zależności od okoliczności czynności przetwarzania); oraz (ii) Dostawca zawrze z każdym zatwierdzonym Podwykonawcą Podmiotu Przetwarzającego pisemne umowy i na żądanie dostarczy Kyndryl kopie takich umów.

(b) Jeśli Dostawca ma siedzibę w Kraju Zapewniającym Odpowiedni Poziom Ochrony, a Kyndryl jest Administratorem Danych niepodlegającym Brytyjskiemu Ogólnemu Rozporządzeniu o Ochronie Danych (w wersji włączonej do prawa brytyjskiego na mocy Ustawy o (Wycofaniu z) Unii Europejskiej z 2018 r.), wówczas Dostawca jako Eksporter niniejszym zawiera z Kyndryl Dodatek(-ki) Brytyjski(e) w celu uzupełnienia Standardowych Klauzul Umownych UE określonych w paragrafie 5.2(b) powyżej.

(c) Jeśli Inni Administratorzy, tacy jak Klienci lub podmioty powiązane, zwrócą się z wnioskiem o przystąpienie do Dodatku(-ów) Brytyjskiego(-ich), Dostawca niniejszym wyraża zgodę na każdy taki wniosek.

(d) Informacje o Załączniku (zgodnie z Tabelą 3) w Dodatku Brytyjskim można znaleźć w odpowiednich Standardowych Klauzulach Umownych UE, niniejszych Warunkach, samym Dokumencie Transakcyjnym oraz związanej z nim umowie podstawowej między stronami. Ani Kyndryl, ani Dostawca nie mogą zakończyć obowiązywania Dodatku(-ów) Brytyjskiego(-ich) w przypadku zmian wprowadzonych do Dodatku(-ów) Brytyjskiego(-ch).

(e) W przypadku jakiejkolwiek sprzeczności pomiędzy Dodatkiem(-ami) Brytyjskim(i) a niniejszymi Warunkami, pierwszeństwo będzie(-ą) mieć Dodatek(-ki) Brytyjski(e).

5.4 W odniesieniu do Serbskich Standardowych Klauzul Umownych:

(a) Jeśli Dostawca nie ma siedziby w Kraju Zapewniającym Odpowiedni Poziom Ochrony, to: (i) Dostawca niniejszym zawiera z Kyndryl Serbskie Standardowe Klauzule Umowne we własnym imieniu jako Podmiot Przetwarzający; oraz (ii) Dostawca zawrze z każdym zatwierdzonym Podwykonawcą Podmiotu Przetwarzającego pisemną umowę przedstawioną w Artykule 8 Serbskich Standardowych Klauzul Umownych i na żądanie dostarczy Kyndryl kopie takich umów.

(b) Jeśli Dostawca ma siedzibę w Kraju Zapewniającym Odpowiedni Poziom Ochrony, to niniejszym Dostawca zawiera z Kyndryl Serbskie Standardowe Klauzule Umowne w imieniu każdego Podwykonawcy Podmiotu Przetwarzającego mającego siedzibę w Kraju Niezapewniającym Odpowiedniego Poziomu Ochrony. Jeśli Dostawca nie może zawrzeć tych klauzul w imieniu któregokolwiek z takich Podwykonawców Podmiotu Przetwarzającego, to wówczas dostarczy Kyndryl Serbskie Standardowe Klauzule Umowne podpisane przez

tego Podwykonawcę Podmiotu Przetwarzającego w celu ich podpisania przez Kyndryl przed zezwoleniem temu Podwykonawcy Podmiotu Przetwarzającego na Przetwarzanie jakichkolwiek Danych Osobowych Kyndryl.

(c) Serbskie Standardowe Klauzule Umowne obowiązujące pomiędzy Kyndryl i Dostawcą będą stanowić Serbskie Standardowe Klauzule Umowne obowiązujące pomiędzy Administratorem a Podmiotem Przetwarzającym lub pisemną umowę typu back-to-back zawartą pomiędzy „podmiotem przetwarzającym" i „podwykonawcą podmiotu przetwarzającego", w zależności od sytuacji. W przypadku sprzeczności między Serbskimi Standardowymi Klauzulami Umownymi a niniejszymi Warunkami znaczenie rozstrzygające będą mieć Serbskie Standardowe Klauzule Umowne.

(d) Informacje wymagane do uzupełnienia Załączników od 1 do 8 Serbskich Standardowych Klauzul Umownych w celu zarządzania przesyłaniem Danych Osobowych do Kraju Niezapewniającego Odpowiedniego Poziomu Ochrony można znaleźć w tych Warunkach, w Załączniku do Dokumentu Transakcyjnego lub w samym Dokumencie Transakcyjnym.

5.5. Dotyczy Dodatku(-ów) Szwajcarskiego(-ich):

(a) Jeżeli, i w odnośnym zakresie, transfer Danych Osobowych Kyndryl zgodnie z paragrafem 5.1. podlega Szwajcarskiej Federalnej Ustawie o Ochronie Danych („FADP") dla Standardowych Klauzul Umownych UE uzgodnionych w paragrafie 5.2., transfer ten będzie podlegał niniejszym Warunkom wraz z poniższymi zmianami w celu zastosowania standardu RODO dla szwajcarskich Danych Osobowych:

- Odniesienia do ogólnego Rozporządzenia o Ochronie Danych Osobowych („RODO") należy rozumieć również jako odniesienia do odpowiednich przepisów w FADP.
- Szwajcarska Federalna Komisja ds. Ochrony Danych jest właściwym organem nadzorczym zgodnie z Klauzulą 13 i Załącznikiem I.C Standardowych Klauzul Umownych UE.
- Szwajcarskie prawo jako obowiązujące dla transferu danych podlega wyłącznie FADP.
- Termin „państwo członkowskie" w Klauzuli 18 Standardowej Klauzuli Umownej UE zostanie rozszerzony o Szwajcarię w celu umożliwienia szwajcarskim obywatelom, których dane są przetwarzane, dochodzenia swoich praw w miejscu zamieszkania.

(b) Dla uniknięcia wątpliwości żadne z powyższych stwierdzeń nie ma na celu obniżenia poziomu ochrony danych zapewnianej przez Standardową Klauzulę Umowną UE w jakikolwiek sposób, ale wyłącznie rozszerzanie tego poziomu ochrony o szwajcarskich obywateli, których dane są przetwarzane. W każdym innym przypadku decydujące znaczenie mają Standardowe Klauzule Umowne UE.

6. Pomoc i rekordy

6.1 Ze względu na charakter Przetwarzania Dostawca udzieli Kyndryl pomocy – poprzez udostępnienie odpowiednich środków technicznych i organizacyjnych – w realizacji zobowiązań dotyczących wniosków i praw Podmiotów Danych. Dostawca zapewni Kyndryl również pomoc w zakresie przestrzegania zobowiązań dotyczących zapewnienia bezpieczeństwa Przetwarzania, powiadamiania o Naruszeniach Bezpieczeństwa i oceny ich skutków dla ochrony danych, w tym, jeśli jest to wymagane, uprzedniej konsultacji z odpowiedzialnym organem regulacyjnym, z uwzględnieniem informacji dostępnych dla Dostawcy.

6.2 Dostawca będzie utrzymywać i aktualizować rekord zawierający nazwę/nazwisko i dane kontaktowe każdego Podwykonawcy Podmiotu Przetwarzającego, w tym każdego przedstawiciela Podwykonawcy Podmiotu Przetwarzającego i inspektora ochrony danych w firmie Podwykonawcy Podmiotu Przetwarzającego. Na żądanie Kyndryl Dostawca udostępni ten rekord Kyndryl w terminie umożliwiającym Kyndryl udzielenie w odpowiednim czasie odpowiedzi na każde żądanie Klienta lub osoby trzeciej.

Artykuł IV. Środki techniczne i organizacyjne. Bezpieczeństwo kodu

Artykuł ten ma zastosowanie, jeśli Dostawca ma dostęp do Kodu Źródłowego Kyndryl. Dostawca będzie przestrzegać wymagań określonych w niniejszym Artykule i w ten sposób chronić Kod Źródłowy Kyndryl przed utratą, zniszczeniem, zmianą, ujawnieniem przypadkowym lub ujawnieniem bez zezwolenia, dostępem przypadkowym lub dostępem bez zezwolenia oraz wszelkimi działaniami niezgodnymi z prawem. Wymagania określone w niniejszym Artykule obowiązują w odniesieniu do wszelkich aplikacji, platform i infrastruktur informatycznych, które Dostawca wykorzystuje w celu świadczenia Usług i udostępniania Produktów Dostarczanych oraz Używania Technologii Kyndryl, w tym wszelkich środowisk programowania, testowania, udostępniania, wsparcia i eksploatacji oraz centrów przetwarzania danych.

1. Wymagania w zakresie bezpieczeństwa

Używane poniżej terminy mają następujące znaczenie:

Kraj Objęty Ograniczeniami oznacza każdy kraj, który: (a) został uznany przez rząd Stanów Zjednoczonych za zagranicznego przeciwnika na mocy rozporządzenia wykonawczego w sprawie zabezpieczenia łańcucha dostaw technologii i usług informatycznych i komunikacyjnych (Executive Order on Securing the Information and Communications Technology and Services Supply Chain) z 15 maja 2019 r.; (b) został umieszczony na liście, o której mowa w paragrafie 1654 amerykańskiej ustawy dotyczącej obrony państwa (National Defense Authorization Act) z 2019 r.; lub (c) został określony jako „Kraj Objęty Ograniczeniami" w Dokumencie Transakcyjnym.

1.1 Dostawca nie będzie dystrybuować Kodu Źródłowego Kyndryl ani umieszczać go w depozycie z korzyścią dla jakiejkolwiek osoby trzeciej.

1.2 Dostawca nie zezwoli, aby jakikolwiek Kod Źródłowy Kyndryl został umieszczony na serwerach znajdujących się w Kraju Objętym Ograniczeniami.Dostawca nie zezwoli jakimkolwiek osobom, w tym członkom swojego Personelu, mającym siedzibę w Kraju Objętym Ograniczeniami lub odwiedzającym Kraj Objęty Ograniczeniami (przez czas trwania takiej wizyty), z jakiejkolwiek przyczyny, na używanie Kodu Źródłowego Kyndryl lub uzyskiwanie do niego dostępu, niezależnie od tego, czy taki Kod Źródłowy Kyndryl jest dostępny globalnie. Dostawca nie zezwoli również w Kraju Objętym Ograniczeniami na programowanie, testowanie lub inne prace, które wymagałyby używania Kodu Źródłowego Kyndryl lub uzyskania do niego dostępu.

1.3 Dostawca nie umieści i nie będzie dystrybuować Kodu Źródłowego Kyndryl w kraju, w którym prawo lub jego interpretacja wymaga ujawniania Kodu Źródłowego osobom trzecim. Jeśli w kraju, w którym został umieszczony Kod Źródłowy Kyndryl, nastąpi zmiana prawa lub jego interpretacji, która może wymagać od Dostawcy ujawnienia takiego kodu osobie trzeciej, to wówczas Dostawca niezwłocznie zniszczy taki Kod Źródłowy Kyndryl lub usunie go z tego kraju oraz nie będzie umieszczać w tym kraju dodatkowego Kodu Źródłowego Kyndryl, dopóki takie prawo lub jego interpretacja pozostanie w mocy.

1.4 Dostawca nie będzie podejmować jakichkolwiek działań, bezpośrednio ani pośrednio, w tym zawierać jakichkolwiek umów, które mogłyby nałożyć na Dostawcę, Kyndryl lub osobę trzecią obowiązek ujawnienia danych na mocy paragrafu 1654 lub 1655 amerykańskiej ustawy dotyczącej obrony państwa (National Defense Authorization Act) z 2019 roku. Dla ścisłości ustala się, że – z wyjątkiem przypadków określonych w Dokumencie Transakcyjnym lub powiązanej z nim umowie podstawowej zawartej między Stronami – Dostawca w żadnych okolicznościach nie może ujawniać Kodu Źródłowego Kyndryl jakimkolwiek osobom trzecim bez uprzedniej pisemnej zgody Kyndryl.

1.5 Jeśli Kyndryl powiadomi Dostawcę lub jeśli osoba trzecia powiadomi którąkolwiek ze Stron, że (a) Dostawca zezwolił na umieszczenie Kodu Źródłowego Kyndryl w Kraju Objętym Ograniczeniami lub kraju, o którym mowa w paragrafie 1.3 powyżej; (b) Dostawca w inny sposób udostępnił Kod Źródłowy Kyndryl, uzyskał do niego dostęp lub użył go w sposób, który nie jest dozwolony w Dokumencie Transakcyjnym bądź powiązanej z nim umowie podstawowej lub innej umowie zawartej między Stronami; lub (c) Dostawca naruszył postanowienia paragrafu 1.4 powyżej, to wówczas, bez ograniczania praw Kyndryl do zastosowania środków przysługujących mu na mocy prawa lub zasad słuszności, Dokumentu Transakcyjnego lub powiązanej z tym

dokumentem umowy podstawowej lub innej umowy zawartej między Stronami, (i) w przypadku gdy takie powiadomienie jest adresowane do Dostawcy, to Dostawca niezwłocznie przekaże je Kyndryl; (ii) Dostawca, zgodnie z uzasadnionymi instrukcjami Kyndryl, zbada sprawę, której dotyczy powiadomienie, i zastosuje w odniesieniu do niej odpowiednie środki naprawcze w rozsądnym czasie wskazanym przez Kyndryl (po konsultacji z Dostawcą).

1.6 Jeśli Kyndryl na podstawie uzasadnionych przesłanek uzna, że zmiany wprowadzone w strategiach, procedurach lub mechanizmach kontrolnych Dostawcy dotyczących dostępu do Kodu Źródłowego są niezbędne w celu zapobieżenia czynnikom ryzyka związanym z cyberbezpieczeństwem, kradzieżą własności intelektualnej lub innym podobnym czynnikom ryzyka (w tym ryzyku, że bez wprowadzenia takich zmian Kyndryl nie będzie mógł sprzedawać produktów i usług określonym Klientom lub na określonych rynkach, bądź w inny sposób nie będzie mógł spełnić wymagań Klienta dotyczących bezpieczeństwa lub funkcjonowania łańcucha dostaw), to wówczas Kyndryl może skontaktować się z Dostawcą w celu omówienia działań niezbędnych do przeciwdziałania takim czynnikom ryzyka, w tym wprowadzenia zmian we wspomnianych strategiach, procedurach lub mechanizmach kontrolnych. Na żądanie Kyndryl Dostawca nawiąże współpracę z Kyndryl w celu oceny zasadności takich zmian oraz ich ewentualnego wprowadzenia po uzgodnieniu przez obie Strony.

Artykuł V. Bezpieczne tworzenie produktów

Niniejszy Artykuł ma zastosowanie, jeśli Dostawca udostępni Kyndryl swój Kod Źródłowy lub Kod Źródłowy osoby trzeciej albo Oprogramowanie Instalowane Lokalnie, bądź jeśli którekolwiek z Usług lub Produktów Dostarczanych Dostawcy będą udostępniane Klientowi Kyndryl jako część produktu lub usługi Kyndryl.

1. Gotowość do zapewnienia bezpieczeństwa

1.1 Dostawca zaangażuje się w procesy wewnętrzne Kyndryl, których celem jest ocena produktów i usług Kyndryl uzależnionych od Produktów Dostarczanych Dostawcy pod względem gotowości do zapewnienia bezpieczeństwa, w tym udzielania we właściwym czasie wyczerpujących odpowiedzi na prośby o informacje za pośrednictwem dokumentów, innych rekordów, wywiadów z odpowiednim Personelem Dostawcy lub w inny sposób.

2. Bezpieczne tworzenie produktów

2.1 Niniejszy paragraf 2 ma zastosowanie wyłącznie w przypadku, gdy Dostawca dostarcza do Kyndryl Oprogramowanie Instalowane Lokalnie.

2.2 Dostawca wdrożył i będzie utrzymywać przez cały okres obowiązywania Dokumentu Transakcyjnego, zgodnie ze Sprawdzonymi Procedurami Branżowymi, strategię bezpieczeństwa oraz procedury i mechanizmy kontroli dotyczące sieci, platformy, systemu, aplikacji, urządzeń, infrastruktury fizycznej, reagowania na incydenty i personelu, które są niezbędne do ochrony: (a) systemów i środowisk programistycznych, kompilacyjnych, testowych i operacyjnych, które Dostawca lub jakakolwiek osoba trzecia zaangażowana przez Dostawcę eksploatuje, którymi zarządza, których używa lub na których w inny sposób polega w odniesieniu do Produktów Dostarczanych, oraz (b) kodu źródłowego wszystkich Produktów Dostarczanych przed utratą, niezgodnymi z prawem formami obsługi oraz nieuprawnionym dostępem, ujawnieniem lub zmianą.

3. Certyfikacja ISO 20243

3.1 Niniejszy paragraf 3 ma zastosowanie wyłącznie w przypadku, gdy którekolwiek z Usług lub Produktów Dostarczanych Dostawcy będą udostępniane Klientowi Kyndryl jako część produktu lub usługi Kyndryl.

3.2 Dostawca uzyska certyfikat zgodności z normą ISO 20243 „Technologia informatyczna – Standard TM Open Trusted Technology Provider (O-TTPS) – Minimalizowanie występowania celowo uszkodzonych i podrobionych produktów" (oparty na ocenie przeprowadzonej samodzielnie lub przez niezależnego rewidenta o dobrej reputacji). Dostawca może też, po złożeniu w tej sprawie pisemnego wniosku, który Kyndryl potwierdzi również w formie pisemnej, uzyskać certyfikat zgodności ze standardem branżowym stanowiącym zasadniczy odpowiednik normy ISO 20243, dotyczący bezpiecznych praktyk projektowania i łańcucha dostaw (oparty na ocenie przeprowadzonej samodzielnie lub przez niezależnego rewidenta o dobrej reputacji, pod warunkiem zatwierdzenia przez Kyndryl).

3.3 Dostawca uzyska certyfikat zgodności z normą ISO 20243 lub merytorycznie równorzędnym standardem branżowym (pod warunkiem pisemnego zatwierdzenia przez Kyndryl) w ciągu 180 dni od daty wejścia w życie Dokumentu Transakcyjnego,
a następnie będzie odnawiać certyfikację co 12 miesięcy (przy czym każde odnowienie będzie dotyczyć aktualnej w danym czasie wersji stosowanego standardu, tj. normy ISO 20243 lub, pod warunkiem pisemnego zatwierdzenia przez Kyndryl, merytorycznie równorzędnego standardu branżowego dotyczący bezpiecznych praktyk projektowania i łańcucha dostaw).

3.4 Na żądanie Dostawca udostępni Kyndryl kopie certyfikatów, do których uzyskania Dostawca jest zobowiązany zgodnie z paragrafami 2.1 oraz 2.2 powyżej.

4. Słabe Punkty Zabezpieczeń

Używane poniżej terminy mają następujące znaczenie:

Poprawki Błędów oznaczają poprawki błędów i wersje programu, które korygują błędy lub wady, w tym Słabe Punkty Zabezpieczeń, w Produktach Dostarczanych.

Środki Łagodzące oznaczają wszelkie znane sposoby zmniejszania lub unikania czynników ryzyka związanych ze Słabym Punktem Zabezpieczeń.

Słaby Punkt Zabezpieczeń oznacza stan na etapie projektowania, kodowania, programowania, implementacji, testowania, eksploatacji, wsparcia, serwisowania lub zarządzania Produktem Dostarczanym, umożliwiający przeprowadzenie ataku, którego skutkiem może być dostęp bez zezwolenia lub wykorzystanie takiego słabego punktu, w tym: (a) dostęp do systemu, przejęcie nad nim kontroli lub zakłócenie jego działania, (b) dostęp do danych, ich usunięcie, zmiana lub wyodrębnienie, bądź (c) zmiana tożsamości, upoważnień lub uprawnień użytkowników lub administratorów. Słaby Punkt Zabezpieczeń może istnieć niezależnie od przypisania do niego identyfikatora CVE (Common Vulnerabilities and Exposures) lub innej oceny bądź oficjalnej klasyfikacji.

4.1 Dostawca oświadcza i gwarantuje, że: (a) do wykrywania Słabych Punktów Zabezpieczeń będzie stosować Sprawdzone Procedury Branżowe, w tym ciągłe statyczne i dynamiczne skanowanie bezpieczeństwa kodu źródłowego aplikacji, skanowanie bezpieczeństwa kodu open source i skanowanie systemu pod kątem słabych punktów zabezpieczeń, oraz (b) będzie spełniać wymagania niniejszych Warunków, aby pomóc w wykrywaniu i korygowaniu Słabych Punktów Zabezpieczeń w Produktach Dostarczanych i we wszystkich aplikacjach, platformach i infrastrukturach informatycznych, w których i poprzez które Dostawca tworzy i udostępnia Usługi i Produkty Dostarczane, a także w zapobieganiu takim Słabym Punktom Zabezpieczeń.

4.2 Jeśli Dostawca zauważy Słaby Punkt Zabezpieczeń w Produkcie Dostarczanym lub takich aplikacjach, platformach lub infrastrukturach informatycznych, to wówczas dostarczy Kyndryl Poprawki Błędów i Środki Łagodzące dla wszystkich wersji i wydań Produktów Dostarczanych zgodnie z Poziomami Istotności i ramami czasowymi wskazanymi w poniższych tabelach:

Poziom Istotności*
Pilny – Słaby Punkt Zabezpieczeń, który stwarza poważne, potencjalnie globalne ryzyko. Kyndryl określa Pilne Słabe Punkty Zabezpieczeń według własnego uznania, niezależnie od oceny CVSS Base Score.

Krytyczny – Słaby Punkt Zabezpieczeń o ocenie CVSS Base Score od 9 do 10,0.
Wysoki – Słaby Punkt Zabezpieczeń o ocenie CVSS Base Score od 7,0 do 8,9.
Średni – Słaby Punkt Zabezpieczeń o ocenie CVSS Base Score od 4,0 do 6,9.
Niski – Słaby Punkt Zabezpieczeń o ocenie CVSS Base Score od 0,0 do 3,9.

Ramy czasowe				
Pilny	***Krytyczny***	***Wysoki***	***Średni***	***Niski***
Maksymalnie 4 dni, zgodnie z decyzją dyrektora Kyndryl ds. bezpieczeństwa informacji	30 Dni	30 Dni	90 Dni	Zgodnie ze Sprawdzonymi Procedurami Branżowymi

* W każdym przypadku, w którym określony Słaby Punkt Zabezpieczeń nie ma jeszcze przypisanej oceny CVSS Base Score, Dostawca zastosuje Poziom Istotności odpowiadający charakterowi danego Słabego Punktu Zabezpieczeń i towarzyszącym mu okolicznościom.

4.3 W przypadku Słabego Punktu Zabezpieczeń, który został publicznie ujawniony i dla którego Dostawca nie udostępnił jeszcze Kyndryl żadnych Poprawek Błędów ani Środków Łagodzących, Dostawca zaimplementuje wszelkie technicznie wykonalne dodatkowe mechanizmy zabezpieczeń, które mogą zniwelować czynniki ryzyka związane z danym Słabym Punktem Zabezpieczeń.

4.4 Jeśli Kyndryl nie jest zadowolony z reakcji Dostawcy na Słaby Punkt Zabezpieczeń w Produkcie Dostarczanym lub jakiejkolwiek aplikacji, platformie lub infrastrukturze, o których była mowa powyżej, wówczas bez szkody dla jakichkolwiek innych praw Kyndryl Dostawca niezwłocznie umożliwi Kyndryl omówienie jego obaw bezpośrednio z wiceprezesem Dostawcy lub menedżerem Dostawcy tego samego szczebla, który odpowiada za dostarczanie Poprawek Błędów.

4.5 Jako przykłady Słabych Punktów Zabezpieczeń można wymienić kod innej firmy lub wycofany z eksploatacji kod open source, które nie otrzymują już poprawek bezpieczeństwa.

Artykuł VI. Dostęp do Systemów Korporacyjnych

Niniejszy Artykuł ma zastosowanie w przypadku, gdy pracownicy Dostawcy mają dostęp do któregokolwiek Systemu Korporacyjnego.

1. Warunki ogólne

1.1 Kyndryl zdecyduje, czy upoważnić pracowników Dostawcy do dostępu do Systemów Korporacyjnych. Jeśli Kyndryl ich upoważni, wówczas Dostawca będzie przestrzegać postanowień niniejszego Artykułu oraz dopilnuje, aby jego pracownicy również przestrzegali postanowień niniejszego Artykułu podczas uzyskiwania takiego dostępu.

1.2 Kyndryl określi środki, za pośrednictwem których pracownicy Dostawcy mogą uzyskać dostęp do Systemów Korporacyjnych, oraz ustali, czy będą mogli używać w tym celu Urządzeń dostarczonych przez Kyndryl lub Dostawcę.

1.3 Pracownicy Dostawcy mogą uzyskiwać dostęp do Systemów Korporacyjnych i używać Urządzeń, które zostały zatwierdzone przez Kyndryl na potrzeby takiego dostępu, wyłącznie w związku ze świadczeniem Usług. Pracownicy Dostawcy nie mogą używać Urządzeń, które zostały zatwierdzone przez Kyndryl na potrzeby takiego dostępu, w celu świadczenia usług na rzecz innych osób lub podmiotów ani w celu uzyskiwania dostępu do jakichkolwiek systemów informatycznych, sieci, aplikacji, serwisów WWW, narzędzi poczty elektronicznej, narzędzi do współpracy lub innych narzędzi Dostawcy lub osoby trzeciej w związku z Usługami.

1.4 Dla ścisłości ustala się, że pracownicy Dostawcy nie mogą używać Urządzeń, które zostały zatwierdzone przez Kyndryl na potrzeby uzyskiwania dostępu do Systemów Korporacyjnych, w celach osobistych (np. nie mogą przechowywać na takich Urządzeniach plików prywatnych, takich jak nagrania muzyczne, filmy wideo czy zdjęcia, ani też uzyskiwać z tych urządzeń dostępu do Internetu w celach prywatnych).

1.5 Pracownicy Dostawcy nie będą kopiować Materiałów Kyndryl dostępnych za pośrednictwem Systemu Korporacyjnego bez uprzedniej pisemnej zgody Kyndryl (nie będą też w żadnym przypadku kopiować Materiałów Kyndryl na przenośne urządzenia pamięci masowej, takie jak pamięci USB lub zewnętrzne dyski twarde).

1.6 Na żądanie Dostawca potwierdzi, do których Systemów Korporacyjnych jego pracownicy mogą uzyskiwać i uzyskali dostęp w określonym przedziale czasu wskazanym przez Kyndryl, z wyszczególnieniem nazwisk pracowników.

1.7 Jeśli którykolwiek z pracowników Dostawcy z dostępem do Systemu Korporacyjnego: (a) nie jest już zatrudniony przez Dostawcę lub (b) nie wykonuje już pracy wymagającej takiego dostępu, Dostawca powiadomi o tym Kyndryl w ciągu dwudziestu czterech (24) godzin. Dostawca we współpracy z Kyndryl dopilnuje, aby prawa dostępu takiego pracownika lub byłego pracownika do Systemów Korporacyjnych zostały natychmiast unieważnione.

1.8 Dostawca niezwłocznie poinformuje Kyndryl o wszelkich faktycznych lub podejrzewanych incydentach dotyczących bezpieczeństwa (takich jak utrata Urządzenia Kyndryl lub Urządzenia Dostawcy bądź uzyskanie dostępu do Urządzenia, danych, materiałów lub innych informacji przez osobę nieuprawnioną) oraz będzie współpracować z Kyndryl podczas badania takich incydentów.

1.9 Dostawca nie może zezwolić pracownikowi swojego agenta, niezależnego wykonawcy lub podwykonawcy na dostęp do Systemu Korporacyjnego bez uprzedniej pisemnej zgody Kyndryl. Jeśli Kyndryl udzieli takiej zgody, to wówczas Dostawca zobowiąże te osoby i ich pracodawców, w formie umowy, do przestrzegania postanowień niniejszego Artykułu w taki sam sposób, jak przestrzegają ich pracownicy

Dostawcy. Dostawca będzie odpowiedzialny wobec Kyndryl za wszelkie działania i zaniechania takich osób lub ich pracodawców w związku z dostępem do Systemu Korporacyjnego.

2. Oprogramowanie Urządzeń

2.1 Dostawca poinstruuje swoich pracowników, aby w odpowiednim czasie zainstalowali na Urządzeniach oprogramowanie, którego Kyndryl wymaga w celu umożliwienia bezpiecznego dostępu do Systemów Korporacyjnych. Dostawca ani jego pracownicy nie będą ingerować w działanie takiego oprogramowania ani w dostępne w nim funkcje zabezpieczeń.

2.2 Dostawca i jego pracownicy będą przestrzegać określonych przez Kyndryl zasad konfiguracji Urządzeń oraz współpracować z Kyndryl w celu zapewnienia, że oprogramowanie będzie działać zgodnie z intencjami Kyndryl. Przykładowo Dostawca nie będzie unieważniać funkcji blokowania serwisów WWW lub automatycznego stosowania poprawek.

2.3 Pracownicy Dostawcy nie mogą udostępniać innym osobom Urządzeń, których używają w celu uzyskiwania dostępu do Systemów Korporacyjnych, ani też stosowanych na tych Urządzeniach nazw użytkowników, haseł i tym podobnych.

2.4 Jeśli Kyndryl upoważni pracowników Dostawcy do uzyskiwania dostępu do Systemów Korporacyjnych za pomocą Urządzeń Dostawcy, to wówczas Dostawca zainstaluje i uruchomi na tych Urządzeniach system operacyjny zatwierdzony przez Kyndryl, a na żądanie Kyndryl w rozsądnym czasie zmieni ten system na nowy lub zaktualizuje go do nowej wersji.

3. Nadzór i współpraca

3.1 Kyndryl ma bezwarunkowe prawo do monitorowania potencjalnych włamań i innych zagrożeń cybernetycznych oraz stosowania w związku z tym czynności naprawczych w dowolny sposób, z każdej lokalizacji i z wykorzystaniem środków, które Kyndryl uzna za niezbędne lub odpowiednie, bez uprzedniego powiadamiania o tym Dostawcy, jego pracowników lub innych osób. W ramach takich praw Kyndryl może w każdej chwili (a) przeprowadzić test bezpieczeństwa dowolnego Urządzenia; (b) monitorować, odzyskiwać za pomocą środków technicznych lub innych środków oraz przeglądać komunikację (w tym wiadomości e-mail z dowolnego konta pocztowego), rekordy, pliki i inne materiały przechowywane w dowolnym Urządzeniu lub przesyłane za pośrednictwem dowolnego Systemu Korporacyjnego; (c) pozyskać pełny obraz każdego Urządzenia na potrzeby badania incydentów. Jeśli w celu korzystania ze swoich praw Kyndryl potrzebuje współpracy ze strony Dostawcy, to Dostawca będzie w pełni i terminowo realizować wnioski Kyndryl o taką współpracę (w tym np. wnioski dotyczące bezpiecznego skonfigurowania Urządzenia, instalacji na Urządzeniu oprogramowania monitorującego lub innego oprogramowania, udostępniania danych o połączeniach na poziomie systemu, stosowania środków reagowania na incydenty na dowolnym Urządzeniu oraz zapewnienia Kyndryl fizycznego dostępu do dowolnego Urządzenia w celu uzyskania pełnego obrazu na potrzeby badania incydentów, a także inne podobne i powiązane wnioski).

3.2 Kyndryl może w każdej chwili unieważnić prawo dostępu do Systemów Korporacyjnych każdemu pracownikowi lub wszystkim pracownikom Dostawcy, bez uprzedniego powiadamiania Dostawcy, jego pracowników lub innych osób, jeśli Kyndryl uzna to za niezbędne w celu zapewnienia sobie bezpieczeństwa.

3.3 Żadne z postanowień Dokumentu Transakcyjnego, powiązanej z nim umowy podstawowej lub innej umowy zawartej między Stronami nie blokuje, nie umniejsza i nie ogranicza w jakikolwiek sposób praw Kyndryl. Dotyczy to w szczególności postanowień wymagających, aby dane, materiały lub inne informacje znajdowały się wyłącznie w określonej lokalizacji lub lokalizacjach, bądź aby tylko osoby z wybranych lokalizacji uzyskiwały dostęp do takich danych, materiałów lub innych informacji.

4. Urządzenia Kyndryl

4.1 Kyndryl zachowuje prawo własności do wszystkich Urządzeń Kyndryl, przy czym Dostawca ponosi ryzyko utraty Urządzeń, w tym na skutek kradzieży, wandalizmu lub zaniedbania. Dostawca nie będzie dokonywać ani zezwalać na dokonywanie jakichkolwiek modyfikacji Urządzeń Kyndryl bez uprzedniej pisemnej zgody Kyndryl, przy czym za modyfikację uważa się każdą zmianę wprowadzoną w Urządzeniu, w tym dowolne zmiany w oprogramowaniu, aplikacjach, projekcie zabezpieczeń, konfiguracji zabezpieczeń bądź projekcie układu fizycznego, mechanicznego lub elektrycznego Urządzenia.

4.2 Dostawca zwróci Kyndryl wszystkie Urządzenia Kyndryl w ciągu 5 dni roboczych po zakończeniu okresu, w którym Urządzenia te są potrzebne do świadczenia Usług, i na żądanie Kyndryl w tym samym czasie zniszczy wszystkie dane, materiały i inne informacje znajdujące się na tych Urządzeniach bez zachowania kopii, zgodnie ze Sprawdzonymi Procedurami Branżowymi, w celu trwałego usunięcia takich danych, materiałów i innych informacji. Dostawca zapakuje i zwróci Urządzenia Kyndryl w takim stanie, w jakim zostały one mu dostarczone (z uwzględnieniem standardowego zużycia), na własny koszt, w miejsce wskazane przez Kyndryl. Niedopełnienie przez Dostawcę zobowiązań określonych w niniejszym paragrafie 4.2 stanowi istotne naruszenie warunków Dokumentu Transakcyjnego oraz powiązanej z nim umowy podstawowej lub innej powiązanej umowy zawartej między Stronami, przy czym umowa jest „powiązana", jeśli dostęp do Systemu Korporacyjnego ułatwia Dostawcy wykonanie zadań lub innych działań określonych w takiej umowie.

4.3 Kyndryl zapewni wsparcie dla Urządzeń Kyndryl (w tym inspekcję Urządzeń oraz serwis prewencyjny i naprawczy). Dostawca niezwłocznie powiadomi Kyndryl o zapotrzebowaniu na serwis naprawczy.

4.4. Kyndryl udziela Dostawcy na czas określony prawa do używania i przechowywania oprogramowania, które stanowi własność Kyndryl lub na które Kyndryl ma prawo udzielać licencji, a także do sporządzenia odpowiedniej liczby kopii takiego oprogramowania na potrzeby używania przez Dostawcę Urządzeń Kyndryl zgodnie z autoryzacją. Dostawca nie może przenosić oprogramowania na inne osoby, tworzyć kopii informacji o licencji na oprogramowanie, dezasemblować, dekompilować lub odtwarzać kodu źródłowego oprogramowania, ani też dokonywać translacji oprogramowania w inny sposób, o ile nie jest to wyraźnie dozwolone przez obowiązujące prawo, bez możliwości wyłączenia w ramach umowy.

5. Aktualizacje

5.1 Bez względu na stanowiące inaczej warunki Dokumentu Transakcyjnego lub powiązanej z nim umowy podstawowej zawartej między Stronami, Kyndryl może, za pisemnym powiadomieniem Dostawcy, ale bez potrzeby uzyskania jego zgody, zaktualizować, uzupełnić lub w inny sposób poprawić niniejszy Artykuł w celu spełnienia wymagań wynikających z obowiązującego prawa lub zobowiązań Klienta, uwzględnienia zmian sprawdzonych procedur dotyczących bezpieczeństwa lub w innym celu, który Kyndryl uzna za niezbędny do ochrony Systemów Korporacyjnych lub Kyndryl.

Artykuł VII. Wspomaganie personelu

Artykuł ten ma zastosowanie w przypadku, gdy pracownicy Dostawcy przeznaczają cały swój czas pracy na świadczenie Usług na rzecz Kyndryl, świadczą wszystkie te Usługi w obiektach Kyndryl, obiektach Klienta lub z własnych domów, a w trakcie ich świadczenia uzyskują dostęp do Systemów Korporacyjnych wyłącznie za pomocą Urządzeń Kyndryl.

1. Dostęp do Systemów Korporacyjnych. Środowiska Kyndryl

1.1 Dostawca może świadczyć Usługi wyłącznie poprzez uzyskiwanie dostępu do Systemów Korporacyjnych za pomocą Urządzeń udostępnionych przez Kyndryl.

1.2 Podczas uzyskiwania dostępu do Systemów Korporacyjnych Dostawca będzie zawsze przestrzegać warunków określonych w Artykule VI (Dostęp do Systemów Korporacyjnych).

1.3 Urządzenia udostępnione przez Kyndryl to jedyne urządzenia, których Dostawca i jego pracownicy mogą używać w celu świadczenia Usług. Z urządzeń tych Dostawca i jego pracownicy mogą korzystać wyłącznie na potrzeby świadczenia Usług. Dla ścisłości ustala się, że Dostawca ani jego pracownicy w żadnym przypadku nie mogą używać innych urządzeń w celu świadczenia Usług, ani też używać Urządzeń Kyndryl na rzecz innego klienta Dostawcy lub w celu innym niż świadczenie Usług na rzecz Kyndryl.

1.4 Pracownicy Dostawcy korzystający z Urządzeń Kyndryl mogą udostępniać sobie nawzajem Materiały Kyndryl i przechowywać je na Urządzeniach Kyndryl, ale tylko w zakresie, w jakim jest to niezbędne do efektywnego świadczenia Usług.

1.5 Z wyjątkiem Materiałów Kyndryl przechowywanych na Urządzeniach Kyndryl w sposób określony powyżej Dostawca ani jego pracownicy w żadnym przypadku nie mogą usuwać Materiałów Kyndryl z repozytoriów, środowisk, narzędzi ani infrastruktur Kyndryl, w których materiały te są przechowywane przez Kyndryl.

1.6 Dla ścisłości ustala się, że Dostawca ani jego pracownicy nie mogą przekazywać Materiałów Kyndryl do repozytoriów, środowisk, narzędzi lub infrastruktur Dostawcy ani też do innych jego systemów, platform czy sieci bez uprzedniej pisemnej zgody Kyndryl.

1.7 Artykuł VIII (Środki techniczne i organizacyjne. Bezpieczeństwo ogólne) nie ma zastosowania do Usług Dostawcy, w przypadku których pracownicy Dostawcy przeznaczają cały swój czas pracy na świadczenie Usług na rzecz Kyndryl, świadczą wszystkie te Usługi w obiektach Kyndryl, obiektach Klienta lub z własnych domów, a w trakcie ich świadczenia uzyskują dostęp do Systemów Korporacyjnych wyłącznie za pomocą Urządzeń Kyndryl. W innych przypadkach Artykuł VIII ma zastosowanie do Usług Dostawcy.

Artykuł VIII. Środki techniczne i organizacyjne. Bezpieczeństwo ogólne

Niniejszy Artykuł ma zastosowanie, jeśli Dostawca świadczy Usługi na rzecz Kyndryl lub udostępnia Kyndryl Produkty Dostarczane, chyba że podczas świadczenia tych Usług i udostępniania Produktów Dostarczanych Dostawca ma dostęp wyłącznie do Biznesowych Informacji Kontaktowych Kyndryl (tzn. nie Przetwarza innych Danych Kyndryl ani nie uzyskuje dostępu do jakichkolwiek innych Materiałów Kyndryl lub jakiegokolwiek Systemu Korporacyjnego), Usługi i Produkty Dostarczane Dostawcy mają na celu udostępnienie Kyndryl Oprogramowania Instalowanego Lokalnie lub Dostawca świadczy wszystkie swoje Usługi i udostępnia Produkty Dostarczane w modelu wspomagania personelu określonym w Artykule VII, w tym w paragrafie 1.7 tego Artykułu.

Dostawca będzie przestrzegać wymagań określonych w niniejszym Artykule i w ten sposób chronić: (a) Materiały Kyndryl przed utratą, zniszczeniem, zmianą, ujawnieniem przypadkowym lub ujawnieniem bez zezwolenia, dostępem przypadkowym lub dostępem bez zezwolenia; (b) Dane Kyndryl przed Przetwarzaniem w sposób niezgodny z prawem; oraz (c) Technologię Kyndryl przed Używaniem w sposób niezgodny z prawem. Wymagania określone w niniejszym Artykule obowiązują w odniesieniu do wszelkich aplikacji, platform i infrastruktur informatycznych, które Dostawca wykorzystuje w celu świadczenia Usług i udostępniania Produktów Dostarczanych oraz Używania Technologii Kyndryl, w tym wszelkich środowisk programowania, testowania, udostępniania, wsparcia i eksploatacji oraz centrów przetwarzania danych.

1. Strategie bezpieczeństwa

1.1 Dostawca będzie utrzymywać i stosować strategie i procedury bezpieczeństwa informatycznego, które są integralną częścią działalności Dostawcy, obowiązują wszystkich członków Personelu Dostawcy i są spójne ze Sprawdzonymi Procedurami Branżowymi.

1.2 Dostawca będzie co najmniej raz na rok dokonywać przeglądu swoich strategii i procedur bezpieczeństwa informatycznego oraz korygować je, jeśli uzna to za niezbędne, w sposób zapewniający ochronę Materiałów Kyndryl.

1.3 Dostawca będzie utrzymywać i spełniać standardowe wymagania w zakresie obowiązkowej weryfikacji wszystkich nowo zatrudnianych pracowników. Rozszerzy też te wymagania na cały Personel Dostawcy i przedsiębiorstwa podporządkowane należące w całości do Dostawcy. Wymagania te obejmują sprawdzanie niekaralności w zakresie dozwolonym przez prawo krajowe, weryfikację tożsamości i wszelkie dodatkowe kontrole, które Dostawca uzna za konieczne. Jeśli Dostawca uzna, że jest to niezbędne, będzie okresowo powtarzać i na nowo weryfikować zgodność z tymi wymaganiami.

1.4 Dostawca zapewni swoim pracownikom coroczne kursy dotyczące bezpieczeństwa i ochrony prywatności. Będzie też co roku wymagać od wszystkich takich pracowników uzyskania certyfikatu potwierdzającego przestrzeganie obowiązujących strategii Dostawcy w zakresie etyki biznesowej, poufności i bezpieczeństwa, zgodnie z postanowieniami kodeksu postępowania Dostawcy lub podobnego dokumentu. Osobom mającym dostęp administracyjny do jakichkolwiek komponentów Usług, Produktów Dostarczanych lub Materiałów Kyndryl, stosownie do roli tych osób oraz świadczonego przez nie wsparcia Usług, Produktów Dostarczanych i Materiałów Kyndryl, Dostawca zapewni dodatkowe szkolenia w dziedzinie strategii i procesów, niezbędne do zachowania wymaganej zgodności i utrzymania niezbędnych certyfikatów.

1.5 Dostawca zaprojektuje zabezpieczenia oraz środki ochrony danych i prywatności, aby chronić Materiały Kyndryl i utrzymywać ich dostępność; obejmuje to implementację, utrzymywanie i zachowanie zgodności ze strategiami i procedurami, które wymagają bezpieczeństwa i prywatności uwzględnionej w projekcie, bezpiecznej inżynierii oprogramowania, a także stosowania bezpiecznych operacji, w odniesieniu do wszelkich Usług i Produktów Dostarczanych oraz do Używania Technologii Kyndryl.

2. Incydenty związane z bezpieczeństwem

2.1 Dostawca będzie utrzymywać i stosować udokumentowane strategie reagowania na incydenty zgodne ze Sprawdzonymi Procedurami Branżowymi dotyczącymi postępowania w przypadku incydentów związanych z cyberbezpieczeństwem.

2.2 Dostawca zbada każdy przypadek uzyskania dostępu do Materiałów Kyndryl bez uprawnień lub ich użycia bez zezwolenia oraz zdefiniuje i będzie realizować odpowiedni plan reagowania.

2.3 Dostawca niezwłocznie (i w każdym przypadku przed upływem 48 godzin) powiadomi firmę Kyndryl o wszelkich wykrytych naruszeniach bezpieczeństwa. Dostawca jest zobowiązany przesłać takie powiadomienie na adres cyber.incidents@kyndryl.com. Dostawca dostarczy firmie Kyndryl żądane (w uzasadnionym zakresie) informacje o naruszeniu bezpieczeństwa, oraz o statusie działań naprawczych i działań w zakresie przywracania, podjętych przez Dostawcę. Informacje takie mogą na przykład obejmować dzienniki pokazujące dostęp do Urządzeń, systemów lub aplikacji uzyskiwany przez użytkowników uprzywilejowanych, użytkowników na prawach administratora i innych użytkowników, a także obrazy Urządzeń, systemów, aplikacji i innych podobnych elementów na potrzeby badania incydentów w zakresie, który jest odpowiedni do naruszenia lub podjętych przez Dostawcę czynności naprawczych oraz działań mających na celu odzyskanie danych.

2.4 Dostawca zapewni Kyndryl uzasadnioną pomoc w spełnieniu wszelkich zobowiązań prawnych (w tym zobowiązań do powiadomienia organów regulacyjnych lub Podmiotów Danych) Kyndryl, przedsiębiorstw afiliowanych Kyndryl, a także Klientów (oraz ich klientów i przedsiębiorstw afiliowanych) w związku z Naruszeniem Bezpieczeństwa.

2.5 Dostawca nie poinformuje ani nie powiadomi żadnej osoby trzeciej, że Naruszenie Bezpieczeństwa bezpośrednio lub pośrednio dotyczy Kyndryl lub Materiałów Kyndryl, chyba że Kyndryl wyrazi na to zgodę na piśmie lub jest to wymagane przez prawo. Dostawca powiadomi Kyndryl na piśmie przed rozpowszechnieniem jakiegokolwiek wymaganego prawem powiadomienia wśród osób trzecich, jeśli takie powiadomienie mogłoby bezpośrednio lub pośrednio ujawnić tożsamość Kyndryl.

2.6 W przypadku Naruszenia Bezpieczeństwa, które wynika z naruszenia przez Dostawcę któregokolwiek z jego zobowiązań określonych w niniejszych Warunkach:

(a) Dostawca będzie odpowiedzialny za wszelkie poniesione przez siebie koszty, a także za rzeczywiste koszty poniesione przez Kyndryl w związku z dostarczeniem powiadomienia o Naruszeniu Bezpieczeństwa stosownym organom regulacyjnym bądź innym organom rządowym i odpowiednim instytucjom branżowym stosującym własne regulacje, mediom (jeśli wymaga tego obowiązujące prawo), Podmiotom Danych, Klientom i innym osobom.

(b) Na żądanie Kyndryl Dostawca uruchomi i będzie prowadzić na własny koszt centrum zgłoszeniowe udzielające odpowiedzi na pytania Podmiotów Danych dotyczące Naruszenia Bezpieczeństwa i jego konsekwencji, przez rok od daty powiadomienia takich Podmiotów Danych o Naruszeniu Bezpieczeństwa lub zgodnie z wymaganiami obowiązujących regulacji dotyczących ochrony danych osobowych, w zależności od tego, która z tych dwóch opcji zapewnia większą ochronę. Kyndryl i Dostawca będą współpracować w celu przygotowania skryptów i innych materiałów, które będą używane przez personel centrum zgłoszeniowego przy udzielaniu odpowiedzi na zapytania. Alternatywnie po pisemnym powiadomieniu Dostawcy Kyndryl może uruchomić i prowadzić własne centrum zgłoszeniowe zamiast centrum zgłoszeniowego Dostawcy. W takim przypadku Dostawca zwróci Kyndryl rzeczywiste koszty poniesione przez Kyndryl w związku z uruchomieniem i prowadzeniem takiego centrum zgłoszeniowego.

(c) Dostawca zwróci Kyndryl rzeczywiste koszty świadczenia usług monitorowania i/lub naprawy historii kredytowej przez rok po dacie powiadomienia o Naruszeniu Bezpieczeństwa wszystkich dotkniętych tym naruszeniem osób fizycznych, które zdecydują się skorzystać z takich usług, lub zgodnie z wymaganiami obowiązujących regulacji dotyczących ochrony danych osobowych, w zależności od tego, która z tych dwóch opcji zapewnia większą ochronę.

3. Bezpieczeństwo fizyczne i kontrola fizycznego dostępu (używany poniżej termin „Obiekt" oznacza lokalizację fizyczną, w której Dostawca udostępnia lub przetwarza Materiały Kyndryl bądź w inny sposób uzyskuje do nich dostęp).

3.1 Dostawca będzie utrzymywać odpowiednie fizyczne mechanizmy kontroli wejścia, takie jak barierki, punkty wejścia kontrolowane za pomocą kart, kamery monitoringu i recepcje obsługiwane przez pracowników, aby chronić Obiekt przed dostępem bez zezwolenia.

3.2 Dostawca ograniczy dostęp, w tym dostęp tymczasowy, do Obiektów oraz obszarów kontrolowanych na ich terenie, zgodnie z funkcjami personelu i potrzebami firmy, oraz zadba o to, aby uzyskanie takiego dostępu wymagało zatwierdzenia osoby upoważnionej. Jeśli Dostawca udzieli komukolwiek tymczasowego prawa dostępu, upoważniony pracownik Dostawcy będzie eskortować takiego gościa na terenie Obiektu i wszelkich obszarów kontrolowanych.

3.3 Aby odpowiednio ograniczyć dostęp do obszarów kontrolowanych na terenie Obiektu, Dostawca zaimplementuje fizyczne mechanizmy kontroli dostępu, w tym wieloskładnikowe mechanizmy kontroli dostępu zgodne ze Sprawdzonymi Procedurami Branżowymi. Dostawca będzie także rejestrować wszelkie próby uzyskania dostępu oraz przechowywać powstałe w ten sposób dzienniki przez co najmniej rok.

3.4 Dostawca odbierze prawo dostępu do Obiektów i obszarów kontrolowanych na terenie Obiektu (a) w momencie, w którym pracownik Dostawcy upoważniony do takiego dostępu odejdzie z przedsiębiorstwa, lub (b) gdy upoważniony pracownik Dostawcy nie ma już powodu wynikającego z potrzeb firmy, aby uzyskiwać taki dostęp. Dostawca będzie przestrzegać formalnych, udokumentowanych procedur odchodzenia pracowników z firmy, obejmujących niezwłoczne usunięcie pracownika z list kontroli dostępu i zwrot fizycznych kart identyfikacyjnych.

3.5 Dostawca zadba o środki ostrożności w celu ochrony infrastruktury fizycznej, która jest wykorzystywana do wsparcia Usług i Produktów Dostarczanych oraz Używania Technologii Kyndryl, przed zagrożeniami środowiskowymi, zarówno występującymi w przyrodzie, jak i spowodowanymi przez człowieka, takimi jak zbyt wysoka temperatura otoczenia, pożar, powódź, nadmierna wilgotność, kradzież i akty wandalizmu.

4. Mechanizmy kontroli przesyłania i separacji danych, uzyskiwania do nich dostępu i wprowadzania w nich zmian

4.1 Dostawca będzie utrzymywać udokumentowaną architekturę zabezpieczeń sieci zarządzanych przez Dostawcę w ramach świadczenia Usług, udostępniania Produktów Dostarczanych oraz Używania Technologii Kyndryl. Dostawca przeprowadzi odrębny przegląd takiej architektury sieci oraz zastosuje środki zaprojektowane z myślą o zapobieganiu połączeniom sieciowym z systemami, aplikacjami i urządzeniami sieciowymi bez zezwolenia, aby zapewnić zgodność ze standardami bezpiecznej segmentacji, izolacji i głębokiej obrony. Dostawca nie może używać technologii bezprzewodowej w ramach udostępniania i obsługi jakichkolwiek Usług Serwerowych. Może natomiast korzystać z komunikacji bezprzewodowej w ramach świadczenia Usług i udostępniania Produktów Dostarczanych oraz Używania Technologii Kyndryl, musi jednak w każdej takiej sieci bezprzewodowej wprowadzić szyfrowanie i wymagać w niej bezpiecznego uwierzytelniania.

4.2 Dostawca będzie utrzymywać środki zaprojektowane z myślą o logicznym odseparowaniu Materiałów Kyndryl oraz zapobieganiu ich ujawnieniu lub uzyskiwaniu do nich dostępu przez osoby bez odpowiedniego zezwolenia. Ponadto Dostawca będzie utrzymywać odpowiednią izolację swoich środowisk produkcyjnych, pozaprodukcyjnych i innych, a jeśli Materiały Kyndryl znajdują się już w środowisku pozaprodukcyjnym lub są do niego przenoszone (na przykład w celu powielenia błędu), to Dostawca zadba o to, aby środki bezpieczeństwa i ochrony prywatności w środowisku pozaprodukcyjnym były równoważne tym w środowisku produkcyjnym.

4.3 Dostawca będzie szyfrować przesyłane i przechowywane Materiały Kyndryl (chyba że wykaże firmie Kyndryl w sposób zadowalający, że szyfrowanie Materiałów Kyndryl podczas przechowywania jest technicznie niewykonalne). Dostawca zaszyfruje także wszelkie ewentualne nośniki fizyczne, takie jak nośniki zawierające pliki kopii zapasowych. Dostawca będzie utrzymywać udokumentowane procedury bezpiecznego generowania, wystawiania, dystrybucji, przechowywania, rotacji, odwoływania, odzyskiwania, tworzenia kopii zapasowych, niszczenia i używania kluczy związanych z szyfrowaniem danych oraz uzyskiwania do nich dostępu. Dostawca zapewni zgodność konkretnych metod szyfrujących używanych do takiego szyfrowania ze Sprawdzonymi Procedurami Branżowymi, takimi jak NIST SP 800-131a.

4.4 Jeśli Dostawca musi mieć dostęp do Materiałów Kyndryl, zastrzeże i ograniczy taki dostęp do minimalnego poziomu niezbędnego do udostępniania i wspierania Usług i Produktów Dostarczanych. Dostawca będzie wymagać, aby taki dostęp, w tym dostęp administracyjny do komponentów bazowych (tzn. dostęp uprzywilejowany), miał charakter indywidualny i uzależniony od funkcji pracownika, a ponadto będzie wymagać zatwierdzenia i regularnej weryfikacji przeprowadzanej przez upoważnionych pracowników

Dostawcy zgodnie z zasadami rozdziału obowiązków. Dostawca będzie utrzymywać środki umożliwiające identyfikację i usuwanie kont nadmiarowych i uśpionych. Dostawca będzie również likwidować konta z dostępem uprzywilejowanym w ciągu 24 (dwudziestu czterech) godzin po odejściu właściciela takiego konta z przedsiębiorstwa lub na żądanie Kyndryl bądź upoważnionego pracownika Dostawcy, np. menedżera właściciela konta.

4.5 Zgodnie ze Standardowymi Procedurami Branżowymi Dostawca będzie utrzymywać środki techniczne wymuszające limit czasu nieaktywnych sesji, blokowanie konta po wielokrotnych nieudanych próbach logowania, uwierzytelnianie za pomocą silnego hasła oraz środki wymagające bezpiecznego przesyłania i przechowywania takich haseł. Dodatkowo Dostawca będzie stosować uwierzytelnianie wieloskładnikowe na potrzeby dostępu uprzywilejowanego do Materiałów Kyndryl bez użycia konsoli.

4.6 Dostawca będzie monitorować korzystanie z dostępu uprzywilejowanego oraz utrzymywać środki zapewniające zarządzanie informacjami związanymi z bezpieczeństwem i zdarzeniami, zaprojektowane z myślą o (a) identyfikowaniu dostępu i aktywności bez uprawnień, (b) umożliwieniu odpowiedniego (również pod względem czasowym) reagowania na taki dostęp i aktywność oraz (c) umożliwieniu przeprowadzania przez Dostawcę, Kyndryl (zgodnie z prawami firmy do weryfikacji określonymi w niniejszych Warunkach oraz prawami do audytu wskazanymi w Dokumencie Transakcyjnym bądź powiązanej z nim umowie podstawowej lub innej powiązanej umowie zawartej między Stronami) i inne podmioty audytów sprawdzających zachowanie zgodności z udokumentowaną strategią Dostawcy.

4.7 Dostawca będzie przechowywać dzienniki, w których zgodnie ze Sprawdzonymi Procedurami Branżowymi będzie rejestrować wszelkie przypadki uzyskiwania dostępu z uprawnieniami administratora, użytkownika lub innego dostępu do systemów używanych podczas świadczenia Usług, udostępniania Produktów Dostarczanych lub Używania Technologii Kyndryl, bądź wykonywania innych czynności na takich systemach używanych podczas świadczenia Usług, udostępniania Produktów Dostarczanych lub Używania Technologii Kyndryl lub w odniesieniu do nich (i na żądanie dostarczy te dzienniki Kyndryl). Dostawca będzie utrzymywać środki zaprojektowane z myślą o ochronie przed dostępem bez uprawnień, modyfikacją i przypadkowym lub celowym zniszczeniem takich dzienników.

4.8 Dostawca będzie utrzymywać zabezpieczenia komputerowe dla posiadanych lub zarządzanych przez siebie systemów, w tym systemów użytkowników końcowych, które Dostawca wykorzystuje podczas świadczenia Usług, udostępniania Produktów Dostarczanych lub Używania Technologii Kyndryl. Zabezpieczenia te będą obejmować: firewalle punktów końcowych, pełne szyfrowanie dysków, technologie wykrywania i reagowania na szkodliwe oprogramowanie i zaawansowane, długotrwałe zagrożenia z użyciem i bez użycia sygnatur, czasowe blokady ekranu i rozwiązania do zarządzania punktami końcowymi, które wymuszają przestrzeganie wymagań dotyczących konfiguracji zabezpieczeń i stosowania poprawek. Ponadto Dostawca zaimplementuje techniczne i operacyjne mechanizmy kontroli, aby mieć pewność, że z sieci Dostawcy mogą korzystać tylko znane i zaufane systemy użytkowników końcowych.

4.9 Zgodnie ze Standardowymi Procedurami Branżowymi Dostawca będzie utrzymywać zabezpieczenia środowisk centrów przetwarzania danych, w których znajdują się lub są przetwarzane Materiały Kyndryl. Zabezpieczenia te będą obejmować środki do wykrywania włamań i zapobiegania im oraz środki przeciwdziałające atakom polegającym na spowodowaniu odmowy usługi i niwelujące ich skutki.

5. Kontrola integralności i dostępności usługi i systemów

5.1 Dostawca: (a) przeprowadzi co najmniej raz na rok ocenę ryzyka dotyczącego bezpieczeństwa i prywatności; (b) przeprowadzi testy bezpieczeństwa i oceny słabych punktów zabezpieczeń, w tym automatyczne skanowanie bezpieczeństwa systemów i aplikacji oraz ręczne etyczne hakerstwo, przed udostępnieniem wersji produkcyjnej i raz na rok w późniejszym okresie w odniesieniu do Usług i Produktów Dostarczanych oraz raz na rok w odniesieniu do Używania Technologii Kyndryl; (c) zatrudni wykwalifikowaną, niezależną osobę trzecią do przeprowadzania testów penetracyjnych zgodnych ze Sprawdzonymi Procedurami Branżowymi co najmniej raz na rok, przy czym będą to testy zarówno automatyczne, jak i ręczne; (d) będzie wykonywać automatyczne zarządzanie i rutynową weryfikację zgodności z wymaganą konfiguracją zabezpieczeń w odniesieniu do każdego komponentu Usług i Produktów Dostarczanych oraz Używania Technologii Kyndryl; a także (e) usunie zidentyfikowane słabe punkty zabezpieczeń lub niezgodności z wymaganą konfiguracją zabezpieczeń w oparciu o powiązane ryzyko, podatność i oddziaływanie. Dostawca

podejmie uzasadnione działania w celu uniknięcia przestoju w funkcjonowaniu Usług podczas ich testowania, oceniania, skanowania i przeprowadzania czynności naprawczych. Na żądanie Kyndryl Dostawca dostarczy Kyndryl pisemne zestawienie ostatnich działań w zakresie testów penetracyjnych. Raport ten będzie zawierać co najmniej nazwę produktu objętego testami, liczbę systemów lub aplikacji objętych testami, daty testów, metody zastosowane podczas testów i ogólne podsumowanie wyników.

5.2 Dostawca będzie utrzymywać strategie i procedury zaprojektowane z myślą o zarządzaniu ryzykiem związanym z wprowadzaniem zmian w Usługach, Produktach Dostarczanych lub Używaniu Technologii Kyndryl. Przed implementacją każdej takiej zmiany, w tym zmiany w odpowiednich systemach, sieciach i komponentach bazowych, Dostawca udokumentuje ją w rejestrowanym żądaniu zmiany obejmującym: (a) opis i przyczynę zmiany; (b) szczegółowe informacje i harmonogram implementacji; (c) deklarację ryzyka opisującą wpływ zmiany na Usługi i Produkty Dostarczane, Materiały Kyndryl lub klientów korzystających z Usług; (d) spodziewane rezultaty; (e) plan wycofania zmiany; (f) zatwierdzenie zmiany przez upoważnionych pracowników Dostawcy.

5.3 Dostawca będzie prowadzić spis wszelkich zasobów informatycznych wykorzystywanych w ramach świadczenia Usług, udostępniania Produktów Dostarczanych oraz Używania Technologii Kyndryl. Dostawca będzie nieprzerwanie monitorować poprawność (w tym moc obliczeniową) i dostępność takich zasobów informatycznych, Usług, Produktów Dostarczanych i Technologii Kyndryl, w tym ich komponentów bazowych, a także zarządzać tą poprawnością i dostępnością.

5.4 Dostawca stworzy wszystkie systemy, wykorzystywane do projektowania lub eksploatacji Usług i Produktów Dostarczanych oraz Używania Technologii Kyndryl, na podstawie predefiniowanych obrazów zabezpieczeń systemów lub założeń dotyczących bezpieczeństwa, które są zgodne ze Sprawdzonymi Procedurami Branżowymi, takimi jak wzorce organizacji Center for Internet Security (CIS).

5.5 Bez uszczerbku dla zobowiązań Dostawcy lub praw Kyndryl wynikających z niniejszego Dokumentu Transakcyjnego lub powiązanej z nim umowy podstawowej zawartej pomiędzy Stronami w odniesieniu do ciągłości biznesowej, Dostawca osobno oceni każdą Usługę i Produkt Dostarczany oraz każdy system informatyczny wykorzystywany do Używania Technologii Kyndryl, pod kątem wymagań w zakresie ciągłości biznesowej i informatycznej oraz usuwania skutków katastrofy zgodnie z udokumentowanymi wytycznymi dotyczącymi zarządzania ryzykiem. Dostawca zadba o to, aby każda taka Usługa, Produkt Dostarczany i system informatyczny były wyposażone – w zakresie opartym na przeprowadzonej ocenie ryzyka – w oddzielnie zdefiniowane, udokumentowane, utrzymywane i weryfikowane raz na rok plany zapewnienia ciągłości biznesowej i informatycznej oraz usuwania skutków katastrofy, zgodne ze Standardowymi Procedurami Branżowymi. Dostawca zadba o to, aby plany te uwzględniały zapewnienie konkretnych czasów odtwarzania określonych w paragrafie 5.6 poniżej.

5.6 Konkretny docelowy okres dopuszczalnej utraty danych oraz docelowy czas odtworzenia w odniesieniu do wszelkich Usług Serwerowych to w obu przypadkach 24 godziny. Jednakże, po otrzymaniu od Kyndryl pisemnego powiadomienia o krótszym docelowym okresie dopuszczalnej utraty danych i docelowym czasie odtworzenia, do których Kyndryl zobowiązał się wobec Klienta, Dostawca niezwłocznie zacznie przestrzegać takiego krótszego docelowego okresu dopuszczalnej utraty danych i docelowego czasu odtworzenia (przy czym za pisemną formę powiadomienia jest też uznawana wiadomość e-mail). Wpływa to na wszystkie inne Usługi świadczone przez Dostawcę na rzecz Kyndryl, dlatego Dostawca zadba o opracowanie planów zapewniania ciągłości biznesowej i usuwania skutków katastrofy z docelowym okresem dopuszczalnej utraty danych i docelowym czasem odtworzenia określonymi w sposób, który pozwoli Dostawcy na zachowanie zgodności ze wszelkimi zobowiązaniami Dostawcy wobec Kyndryl określonymi w Dokumencie Transakcyjnym i powiązanej z nim umowie podstawowej zawartej pomiędzy Stronami oraz w niniejszych Warunkach, w tym z jego zobowiązaniami do terminowego zapewniania testów, wsparcia i serwisowania.

5.7 Dostawca będzie utrzymywać środki zaprojektowane z myślą o ocenie, testowaniu i stosowaniu poprawek dotyczących bezpieczeństwa dla Usług i Produktów Dostarczanych oraz powiązanych z nimi systemów, sieci, aplikacji i komponentów bazowych w obrębie takich Usług i Produktów Dostarczanych, a także systemów sieci, aplikacji i komponentów bazowych wykorzystywanych do Używania Technologii Kyndryl. Po uznaniu, że dana poprawka dotycząca bezpieczeństwa jest odpowiednia i stosowna, Dostawca zaimplementuje

ją zgodnie z udokumentowanym poziomem istotności i wytycznymi dotyczącymi oceny ryzyka. Dostawca będzie implementować poprawki dotyczące bezpieczeństwa zgodnie ze swoją strategią zarządzania zmianami.

5.8 Jeśli Kyndryl ma uzasadnione podstawy, aby przypuszczać, że sprzęt lub oprogramowanie dostarczane Kyndryl przez Dostawcę mogą zawierać elementy inwazyjne, takie jak oprogramowanie szpiegujące, szkodliwe oprogramowanie lub złośliwy kod, to wówczas Dostawca niezwłocznie nawiąże współpracę z Kyndryl w celu zbadania podstaw takiego przypuszczenia oraz ewentualnego zastosowania czynności naprawczych.

6. Udostępnianie usług

6.1 Dostawca będzie obsługiwać powszechne w branży metody uwierzytelniania stowarzyszonego dla kont użytkowników Kyndryl lub kont Klienta, przy czym będzie uwierzytelniać takie konta użytkowników Kyndryl lub konta Klienta zgodnie ze Sprawdzonymi Procedurami Branżowymi, poprzez centralnie zarządzane przez Kyndryl wieloskładnikowe pojedyncze logowanie, z użyciem interfejsu OpenID Connect lub protokołu SAML (Security Assertion Markup Language).

7. Podwykonawcy. Z zastrzeżeniem obowiązków Dostawcy lub praw Kyndryl określonych w Dokumencie Transakcyjnym lub powiązanej z nim umowie podstawowej zawartej pomiędzy Stronami, dotyczących zatrzymania podwykonawców, Dostawca zadba o to, aby każdy podwykonawca wykonujący dla niego jakiekolwiek prace stosował mechanizmy kontroli i nadzoru w celu zachowania zgodności z wymaganiami i zobowiązaniami, jakie niniejsze Warunki nakładają na Dostawcę.

8. Nośniki fizyczne. Dostawca będzie bezpiecznie oczyszczać nośniki fizyczne przeznaczone do ponownego wykorzystania przed ich ponownym wykorzystaniem oraz zniszczy nośniki fizyczne nieprzeznaczone do ponownego wykorzystania, zgodnie ze Sprawdzonymi Procedurami Branżowymi dotyczącymi oczyszczania nośników.

Artykuł IX. Certyfikaty i raporty dotyczące Usług Serwerowych

Niniejszy Artykuł ma zastosowanie, jeśli Dostawca świadczy Usługi Serwerowe na rzecz Kyndryl.

1.1 Dostawca uzyska poniższe certyfikaty lub raporty z zachowaniem ram czasowych określonych poniżej:

Certyfikaty i raporty	**Ramy czasowe**
W odniesieniu do Usług Serwerowych świadczonych przez Dostawcę: Certyfikaty zgodności z normą ISO 27001 „Technologia informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji”, oparte na ocenie przeprowadzonej przez niezależnego rewidenta o dobrej reputacji **lub** SOC 2 typu 2 – raport sporządzony przez niezależnego rewidenta o dobrej reputacji, dokumentujący przeprowadzony przegląd systemów, mechanizmów kontroli i operacji Dostawcy zgodnie ze standardem SOC 2 typu 2 (z uwzględnieniem co najmniej bezpieczeństwa, poufności i dostępności).	Dostawca uzyska certyfikację ISO 27001 w ciągu 120 Dni od daty wejścia w życie Dokumentu Transakcyjnego* lub Daty Przyjęcia** oraz będzie odnawiać certyfikację opartą na ocenie przeprowadzonej przez niezależnego rewidenta o dobrej reputacji co 12 miesięcy w późniejszym okresie (przy czym każde odnowienie będzie dotyczyć aktualnej w danym czasie wersji standardu). Dostawca uzyska raport SOC 2 typu 2 w ciągu 240 Dni od daty wejścia w życie Dokumentu Transakcyjnego* lub Daty Przyjęcia**, a następnie w późniejszym czasie będzie co 12 miesięcy uzyskiwać nowy raport sporządzany przez niezależnego rewidenta o dobrej reputacji, dokumentujący przeprowadzony przegląd systemów, mechanizmów kontroli i operacji Dostawcy zgodnie ze standardem SOC 2 typu 2 (z uwzględnieniem co najmniej bezpieczeństwa, poufności i dostępności). * Jeśli Dostawca świadczy Usługę Serwerową od daty wejścia w życie. ** Dzień, w którym Dostawca przyjmuje zobowiązanie do świadczenia Usługi Serwerowej.

1.2 Na pisemny wniosek Dostawcy, zatwierdzony przez Kyndryl również w formie pisemnej, Dostawca może uzyskać certyfikat lub raport stanowiący zasadniczy odpowiednik certyfikatu lub raportu określonego powyżej, przy czym ramy czasowe określone w powyższej tabeli obowiązują bez zmian.

1.3 Dostawca: (a) na żądanie niezwłocznie dostarczy Kyndryl kopię każdego certyfikatu i raportu, którego uzyskanie jest obowiązkiem Dostawcy, (b) niezwłocznie wyeliminuje wszelkie słabe punkty wykryte w trakcie kontroli wewnętrznej i odnotowane podczas przeglądu SOC 2 lub przeglądu stanowiącego jego zasadniczy odpowiednik (zatwierdzony przez Kyndryl).

Artykuł X. Współpraca, weryfikacja i czynności naprawcze

Niniejszy Artykuł ma zastosowanie, gdy Dostawca świadczy Usługi na rzecz Kyndryl lub udostępnia Kyndryl Produkty Dostarczane.

1. Współpraca Dostawcy z Kyndryl

1.1 Jeśli Kyndryl ma podstawy, aby przypuszczać, że jakiekolwiek Usługi lub Produkty Dostarczane spowodowały, powodują lub mogą spowodować problemy dotyczące cyberbezpieczeństwa, to Dostawca będzie w rozsądnym zakresie współpracować z Kyndryl w celu zbadania, czy przypuszczenia te są uzasadnione, w tym będzie udzielać we właściwym czasie wyczerpujących odpowiedzi na prośby o informacje za pośrednictwem dokumentów, innych rekordów, wywiadów z odpowiednim Personelem Dostawcy lub w inny sposób.

1.2 Każda ze Stron zgadza się: (a) na żądanie drugiej Strony udostępnić jej takie dodatkowe informacje; (b) sporządzić i udostępnić drugiej Stronie takie dokumenty; (c) podejmować inne działania, których druga Strona może zażądać na uzasadnionej podstawie, na potrzeby realizacji celów określonych w niniejszych Warunkach oraz przywołanych w nich dokumentach. Przykładowo, na żądanie Kyndryl Dostawca w wymaganym terminie udostępni warunki dotyczące bezpieczeństwa i ochrony prywatności określone w zawartych przez siebie pisemnych kontraktach z Podwykonawcami Podmiotu Przetwarzającego i podwykonawcami, w tym, o ile Dostawca ma takie prawo, poprzez udzielenie Kyndryl dostępu do tych kontraktów.

1.3 Na żądanie Kyndryl Dostawca w wymaganym terminie udostępni informacje na temat krajów, w których jego Produkty Dostarczane i ich komponenty zostały wyprodukowane, zaprojektowane lub pozyskane w inny sposób.

2. Weryfikacja (używany poniżej termin „Obiekt" oznacza lokalizację fizyczną, w której Dostawca udostępnia lub przetwarza Materiały Kyndryl bądź w inny sposób uzyskuje do nich dostęp)

2.1 Dostawca będzie prowadzić podlegający audytowi rejestr na potrzeby wykazania zgodności z niniejszymi Warunkami.

2.2 Kyndryl może, samodzielnie lub za pośrednictwem audytora zewnętrznego, za pisemnym powiadomieniem Dostawcy z wyprzedzeniem 30 dni, zweryfikować przestrzeganie niniejszych Warunków przez Dostawcę. Może to zrobić poprzez uzyskanie dostępu do dowolnego Obiektu lub Obiektów, ale nie uzyska dostępu do żadnego z centrów przetwarzania danych, w których Dostawca Przetwarza Dane Kyndryl, chyba że ma oparte na dobrej wierze podstawy, aby uważać, że w ten sposób pozyskałby wymagane informacje. Podczas takiej weryfikacji Dostawca będzie współpracować z Kyndryl, w tym będzie udzielać we właściwym czasie wyczerpujących odpowiedzi na prośby o informacje za pośrednictwem dokumentów, innych rekordów, wywiadów z odpowiednim Personelem Dostawcy lub w inny sposób.Dostawca może przedstawić Kyndryl dowód przestrzegania zatwierdzonych zasad postępowania lub zgodności z certyfikatem branżowym bądź dostarczyć inne informacje w celu wykazania zgodności z niniejszymi Warunkami.

2.3 Weryfikacja taka będzie się odbywać nie częściej niż raz na 12 miesięcy, chyba że (a) Kyndryl weryfikuje czynności naprawcze zastosowane przez Dostawcę w odniesieniu do problemów, które zostały stwierdzone podczas poprzedniej weryfikacji w trakcie 12-miesięcznego okresu, lub (b) miało miejsce Naruszenie Bezpieczeństwa, a Kyndryl chce zweryfikować realizację zobowiązań dotyczących takiego naruszenia. W każdym przypadku Kyndryl powiadomi Dostawcę na piśmie z takim samym 30-dniowym wyprzedzeniem, jak określono w paragrafie 2.2 powyżej, jeśli jednak Naruszenie Bezpieczeństwa wymaga pilnego podjęcia działań, Kyndryl może przeprowadzić weryfikację za pisemnym powiadomieniem Dostawcy z wyprzedzeniem mniejszym niż 30 dni.

2.4. Organ regulacyjny lub inny Administrator może korzystać z tych samych praw, co Kyndryl, określonych w paragrafach 2.2 i 2.3, przy czym organowi regulacyjnemu mogą również przysługiwać z mocy prawa inne, dodatkowe uprawnienia.

2.5 Jeśli Kyndryl ma uzasadnione podstawy, aby sądzić, że Dostawca narusza którykolwiek z niniejszych Warunków (niezależnie od tego, czy podstawy te wynikają z weryfikacji przeprowadzonej zgodnie z niniejszymi Warunkami, czy z innych przyczyn), to wówczas Dostawca niezwłocznie naprawi skutki takiego naruszenia.

3. Program walki z podróbkami

3.1 Jeśli Produkty Dostarczane Dostawcy obejmują komponenty elektroniczne (np. dyski twarde, dyski SSD, pamięć, procesory, urządzenia logiczne lub kable), to Dostawca będzie realizować udokumentowany program walki z podróbkami, którego celem jest przede wszystkim niedopuszczenie do sytuacji, w której Dostawca dostarczyłby Kyndryl podrobione komponenty, a ponadto szybkie wykrywanie przypadków nieumyślnego dostarczenia Kyndryl przez Dostawcę podrobionych komponentów oraz zastosowanie w związku z tym odpowiednich czynności naprawczych. Dostawca nałoży takie samo zobowiązanie do realizowania udokumentowanego programu walki z podróbkami na wszystkich swoich dostawców, którzy dostarczają komponenty elektroniczne włączone w Produkty Dostarczane udostępniane przez Dostawcę firmie Kyndryl.

4. Czynności naprawcze

4.1 Jeśli Dostawca nie wypełni któregokolwiek ze swoich zobowiązań wynikających z niniejszych Warunków i spowoduje to Naruszenie Bezpieczeństwa, to wówczas Dostawca skoryguje swoje działania i naprawi szkody zaistniałe na skutek Naruszenia Bezpieczeństwa zgodnie z uzasadnionymi instrukcjami Kyndryl oraz w określonym przez Kyndryl terminie. Jeśli jednak Naruszenie Bezpieczeństwa jest wynikiem świadczenia przez Dostawcę Usługi Serwerowej dla wielu użytkowników i w konsekwencji ma wpływ na wielu klientów Dostawcy, w tym Kyndryl, to wówczas Dostawca, biorąc pod uwagę charakter Naruszenia Bezpieczeństwa, terminowo i odpowiednio skoryguje nieprawidłowości w działaniu i usunie szkodliwe skutki Naruszenia Bezpieczeństwa, jednocześnie uwzględniając wszelkie uwagi Kyndryl dotyczące takich korekt i działań naprawczych. Bez uszczerbku dla powyższych ustaleń, Dostawca musi niezwłocznie powiadomić Kyndryl o sytuacji, w której nie może dłużej realizować zobowiązań wynikających z obowiązujących przepisów ochrony danych.

4.2 Kyndryl będzie mieć prawo do uczestniczenia w usuwaniu wszelkich Naruszeń Bezpieczeństwa, o których mowa w paragrafie 4.1, jeśli uzna to za stosowne lub konieczne, a Dostawca będzie odpowiedzialny za swoje koszty i wydatki związane z korektą swoich działań oraz za koszty i wydatki związane z usuwaniem naruszeń, które Strony poniosą w związku z takim Naruszeniem Bezpieczeństwa.

4.3 Przykładowo koszty czynności naprawczych zastosowanych w związku z Naruszeniem Bezpieczeństwa mogą obejmować wykrycie i zbadanie tego naruszenia, określenie obowiązków wynikających z przepisów prawa i regulacji, powiadomienia o Naruszeniu Bezpieczeństwa, utworzenie i prowadzenie centrów zgłoszeniowych, świadczenie usług monitorowania i naprawy historii kredytowej, ponowne załadowanie danych, korygowanie defektów produktów (w tym za pośrednictwem Kodu Źródłowego lub w inny sposób), zaangażowanie osób trzecich do pomocy w wyżej wymienionych lub innych powiązanych czynnościach, a także inne koszty i wydatki niezbędne w celu naprawy szkód wynikających z Naruszenia Bezpieczeństwa. Dla ścisłości ustala się, że koszty czynności naprawczych nie obejmują utraty przez Kyndryl zysków, transakcji, wartości, przychodów, reputacji (goodwill) ani spodziewanych oszczędności.