

POLITYKA: POLITYKA PRYWATNOŚCI DLA PRACOWNIKÓW I OSÓB UBIEGAJĄCYCH SIĘ O PRACĘ

Ostatnia aktualizacja: 15 marca 2026 r.

Witamy! Niniejsza Polityka Prywatności („Polityka”) opisuje w jaki sposób firma Convergent, w tym jej spółki zależne i powiązane, gromadzą, wykorzystują, przechowują i ujawniają Dane osobowe (zdefiniowane poniżej) Pracowników i osób ubiegających się o pracę. Do celów Polityki „Spółka” lub „my” oznacza właściwy podmiot Convergent, który zatrudnia pracownika lub w którym osoba ubiega się o pracę. „Pracownik” oznacza:

- byłych i obecnych pracowników Spółki;
- byłych i obecnych konsultantów, niezależnych wykonawców i pośredników Spółki;
- osoby ubiegające się o pracę, kandydatów i osoby polecane;
- pracowników tymczasowych lub kontraktowych;
- emerytów; oraz
- byłych i obecnych dyrektorów i kierowników Spółki.

Niniejsza Polityka nie ma zastosowania do:

- danych gromadzonych przez Spółkę od osób niebędących Pracownikami lub gromadzonych od Pracowników w kontekście niezwiązanym z zatrudnieniem. W takich sytuacjach prosimy zapoznać się z naszą Polityką prywatności stron trzecich, dostępną pod adresem <https://www.convergent.com/privacy/>.

Convergent jest globalną grupą podmiotów, w związku z czym niniejsza polityka zawiera treści dotyczące konkretnych jurysdykcji.

- Załącznik 1 zawiera [dodatkowe informacje dotyczące Pracowników z Kalifornii](#), w tym nasz Komunikat o gromadzeniu danych.
- Załącznik 2 zawiera [dodatkowe informacje dotyczące Pracowników z Kanady](#).
- Załącznik 3 zawiera [dodatkowe informacje dotyczące Pracowników z Wielkiej Brytanii, Unii Europejskiej i Szwajcarii](#).
- Załącznik 4 zawiera [dodatkowe informacje dotyczące Pracowników z Azji](#).
- Załącznik 5 zawiera [dodatkowe informacje dotyczące Pracowników z Oceanii](#).
- Załącznik 6 zawiera [dodatkowe informacje dotyczące Pracowników w krajach Ameryki Łacińskiej \(Argentyna, Chile, Kolumbia, Meksyk i Brazylia\)](#).
- Załącznik 7 zawiera [dodatkowe informacje dotyczące Pracowników na Bliskim Wschodzie](#).

Mieszkańcy innych regionów mogą kontaktować się z nami pod adresem dataprotectionofficer@convergent.com w przypadku jakichkolwiek pytań dotyczących sposobu przetwarzania danych osobowych.

1. JAK GROMADZIMY DANE OSOBOWE, JAKIE DANE OSOBOWE PRZETWARZAMY I JAK WYKORZYSTUJEMY DANE OSOBOWE

Jak gromadzimy Dane osobowe

„Dane osobowe” oznaczają wszelkie informacje, które identyfikują, odnoszą się do, opisują lub mogą być w uzasadniony sposób powiązane, bezpośrednio lub pośrednio, z zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną lub które są w inny sposób zdefiniowane jako dane osobowe, informacje osobowe lub podobne terminy zgodnie z obowiązującymi przepisami dotyczącymi prywatności lub ochrony danych. Spółka gromadzi niektóre kategorie Danych



osobowych bezpośrednio od Pracowników (na przykład dane dotyczące ubiegania się o pracę, dane kontaktowe i informacje na temat historii zatrudnienia), a inne tworzy (na przykład oceny wyników i rejestry nieobecności). Możemy również gromadzić Dane osobowe od stron trzecich, takich jak agencje rekrutacyjne lub podmioty, które polecają Pracownika na stanowiska lub platformy mediów społecznościowych, portale z ofertami pracy lub podobne strony internetowe, na których Pracownik zamieścił swoje informacje (np. LinkedIn). W niektórych przypadkach gromadzone przez nas Dane osobowe zostały wywnioskowane na podstawie innych informacji przekazanych nam przez Pracownika, uzyskanych w wyniku interakcji z nami lub pochodzących od stron trzecich.

Niektóre informacje są niezbędne, aby umożliwić Spółce rozpatrzenie podania o pracę i/lub zawarcie i administrowanie umową o pracę z Pracownikiem, a Pracownik ma obowiązki wynikające z umowy o pracę, które wymagają przetwarzania niektórych Danych osobowych. Jeśli Pracownik nie poda niezbędnych informacji, utrudni to Spółce zarządzanie prawami i obowiązkami istotnymi dla naszego stosunku pracy. Pracownik może również być zobowiązany do przekazania Spółce danych osobowych w celu skorzystania z przysługujących mu praw ustawowych, takich jak prawo do urlopu ustawowego. Niepodanie takich danych osobowych może oznaczać, że Pracownik nie będzie mógł skorzystać ze swoich praw ustawowych.

Jakie Dane osobowe przetwarzamy

Kategorie Danych osobowych Pracowników przetwarzanych przez Spółkę to:

- Dane osobowe i informacje kontaktowe, takie jak imię i nazwisko, adres e-mail i numer telefonu, adres domowy, data urodzenia, numery ubezpieczenia, numery identyfikacyjne (w tym numery identyfikacyjne wydane przez rząd, np. numer ubezpieczenia społecznego), płeć, stan cywilny, osoby pozostające na utrzymaniu, informacje kontaktowe w nagłych wypadkach i zdjęcia;
- Identyfikatory, takie jak identyfikatory internetowe (np. pliki cookie i adresy IP) emblematy oraz zdjęcia lub skany odcisków palców do celów identyfikacji, weryfikacji, pracownicze numery identyfikacyjne lub numery wydawane do celów bezpieczeństwa / kontroli dostępu.
- Dane dotyczące listy płac i wynagrodzeń, takie jak informacje o danych bankowych, wynagrodzeniu, premiach, świadczeniach, dodatkach do wynagrodzenia na rzecz osób pozostających na utrzymaniu i innych nagród oraz podatkach
- Dane dotyczące prawa do pracy i dane imigracyjne, takie jak status obywatelstwa, dane paszportowe, dane z dowodu osobistego, szczegóły dotyczące pozwolenia na pobyt lub pracę;
- Dane dotyczące zdolności, rekrutacji i ubiegania się o pracę, takie jak informacje o aplikacji lub w niej zawarte, życiorysy/CV, listy polecające, weryfikacje życiorysu zawodowego, odniesienia, wykształcenie, kwalifikacje zawodowe, umiejętności, języki, oceny pracy, plany rozwoju i preferencje dotyczące pracy;
- Informacje o zatrudnieniu i doświadczeniu, w tym opis obecnego stanowiska i poprzednich stanowisk, tytuły, wynagrodzenia, wydziały, lokalizacje, przełożeni, pośredni i bezpośredni podwładni, historia pracy, status i rodzaj zatrudnienia, warunki zatrudnienia, data ponownego zatrudnienia i rozwiązania stosunku pracy, uprawnienia emerytalne, awanse i rejestry działań dyscyplinarnych;
- Dane dotyczące harmonogramu pracy, takie jak rejestry czasu pracy, w tym ewidencja urlopów, zwolnień chorobowych i innych nieobecności, status urlopu, przepracowane godziny, nadgodziny i praca zmianowa;



- Dane medyczne, dotyczące wypadków i zdrowia, w związku z bezpieczeństwem i higieną pracy, świadczeniami oraz administracją wynagrodzeniem pracownika
- Dane administracyjne dotyczące świadczeń, takie jak dane osobowe niezbędne do zarządzania świadczeniami, w tym zdrowotnymi, emerytalnymi, ubezpieczeniowymi i innymi, które możemy każdorazowo oferować Pracownikom;
- Informacje dotyczące podróży, takie jak rezerwacje, trasy podróży, numery wydane przez rząd i preferencje w związku z podróżami; oraz
- Wnioski wyciągnięte z innych Danych osobowych takie jak wnioski, które dotyczą wyników danej osoby w pracy.
- Inne Wrażliwe dane osobowe, dalej opisano w niniejszej Polityce, w tym w części "Wrażliwe dane osobowe."
- Inne informacje podane przez Pracownika podczas ubiegania się o pracę, wdrożenia do pracy lub zatrudnienia.

W niektórych jurysdykcjach możemy pozyskiwać Dane osobowe za pośrednictwem urzędów i pojazdów, które posiada Spółka lub za pośrednictwem urzędów osobistych lub pojazdów, które Pracownik użytkuje do celów służbowych. Nie wszystkie te działania są prowadzone we wszystkich regionach, w tym w miejscach, gdzie są zabronione przepisami prawa, a my pozyskujemy zgodę Pracownika przed rozpoczęciem gromadzenia takich danych tam, gdzie taka zgoda jest wymagana przepisami prawa. Informacje dotyczące szczegółowych praktyk w regionie Pracownika można uzyskać pod adresem dataprotectionofficer@convergint.com.

- Urządzenia śledzące GPS mogą być wykorzystywane w pojazdach zarządzanych przez Spółkę do celów śledzenia czasu pracy Pracownika, związanych z konserwacją pojazdów, wysyłką i planowaniem, promowaniem bezpiecznych praktyk jazdy, audytem, ograniczaniem oszustw, kontrolą kosztów paliwa oraz analizą wskaźników związanych z działalnością biznesową. Podczas użytkowania urządzenia śledzące GPS mogą dostarczać Spółce informacje takie jak lokalizacja pojazdu, trasy przejazdu i prędkość pojazdu, korzystania z pojazdu poza godzinami pracy, czas bezczynności, ingerencja w działanie czujnika, czas uruchomienia i zatrzymania pojazdu oraz czas przyjazdu i odjazdu.
- Dodatkowo pojazdy dostarczane przez Spółkę mogą być również wyposażone w system nagrywania wideo obejmujący kamery (znane również jako „Wideorejestratory”). Są one wykorzystywane, by promować bezpieczeństwo, chronić mienie Spółki i zapobiegać oszukańczemu lub bezprawnemu postępowaniu. Wideorejestratory mogą zbierać informacje takie jak rejestracja pojazdu, nagrania z wideorejestratora, dane z czujnika pobrane przez wideorejestrator związane z działaniem pojazdu oraz interakcje pracowników z systemem wideorejestraora.
- Monitorowanie lokalizacji GPS urządzenia mobilnego Pracownika może być wykorzystywane w celu obsługi programów zwrotu kosztów podróży w przypadku korzystania z pojazdów osobistych w celach służbowych. Zgromadzone dane są ograniczone do danych istotnych dla kalkulacji związanych ze zwrotem kosztów podróży. Pracownik może mieć również możliwość ręcznego zgłaszania informacji dotyczących zwrotu kosztów podróży.
- Niektóre lokalizacje Spółki monitorują zakłady pracy za pomocą kamer wideo w celu zapewnienia bezpieczeństwa i ochrony.
- Rozmowy telefoniczne mogą być monitorowane, jeśli zachodzą interakcje z personelem spółki, klientem lub innym partnerem biznesowym, lub osobą publiczną, w tym obsługą klienta, w celach szkoleniowych, ewidencyjnych i na potrzeby audytu.
- Spotkania mogą być nagrywane lub spisywane w celach dotyczących produktywności i ewidencyjnych, w tym w celu późniejszej weryfikacji przez innych Pracowników i na

convergi^{int}

potrzeby automatycznego tworzenia podsumowań spotkań lub notatek.

- Podczas korzystania z laptopów, tabletów, telefonów komórkowych lub sieci i serwerów Spółki (zwanymi łącznie „Urządzeniami”) do celów związanych ze Spółką, może ona uzyskiwać dostęp do zawartości Urządzeń i monitorować działalność Urządzeń zgodnie ze swoimi politykami, w tym bez ograniczeń monitorować pliki, wiadomości e-mail, czaty, wiadomości na komunikatorach (np. Slack, Teams itp.), aktywności użytkownika i historię przeglądania.

Wszelkie rozmowy telefoniczne, wszelka poczta elektroniczna lub wszelki dostęp do Internetu za pomocą dowolnego urządzenia elektronicznego lub systemu używanego do celów służbowych lub podłączonego do systemów lub sieci służbowych, w tym między innymi korzystanie z komputera, telefonu lub urządzenia mobilnego, mogą podlegać monitorowaniu lub przeglądowi za pomocą wszelkich zgodnych z prawem środków zgodnych z polityką Spółki.

Jak przetwarzamy Dane osobowe

Spółka wykorzystuje Dane osobowe Pracowników do następujących celów:

- Rekrutacja: Przyjmowanie kandydatów i wniosków; ocena przydatności do pełnienia określonych funkcji; komunikowanie się z kandydatami w sprawie wniosków i możliwości zatrudnienia. Możemy komunikować się z kandydatami za pośrednictwem kanałów odpowiadających informacjom podanym przez kandydatów — np. poprzez e-mail, telefon lub SMS-y / wiadomości tekstowe. W przypadku, gdy określone rodzaje komunikacji wymagają zgody zgodnie z obowiązującym prawem, uzyskamy taką zgodę.
- Weryfikacja kandydatów: przeprowadzanie rozmów kwalifikacyjnych, selekcji, ocen i sprawdzanie przeszłości, w tym wykorzystanie technologii automatycznych i uczenia maszynowego (takich jak technologie oparte na sztucznej inteligencji) do analizy danych osobowych kandydatów oraz zwiększenia wydajności i skuteczności przeglądu i analizy zasobów ludzkich. Nie podejmujemy decyzji mających skutki prawne lub podobne znaczenie wyłącznie w oparciu o automatyzację.
- Wdrażanie osób ubiegających się o pracę: potwierdzanie statusu prawnego i prawa do zatrudnienia, ustalanie płac i podatków.
- Zarządzanie siłą roboczą: zarządzanie działaniami w pracy i personelem, w tym zarządzanie i alokacja aktywów Spółki, analiza i planowanie siły roboczej, działalność i operacje w zakresie zasobów ludzkich, biznes i strategiczne planowanie oraz zarządzanie, audyty i sprawozdawczość, zarządzanie finansami i sprawozdawczość finansowa, prowadzenie działalności z klientami, dostawcami i innymi partnerami, ewaluacje i oceny wyników, awanse i przejmowanie stanowisk, administracja płac, premii, dodatków do wynagrodzenia na rzecz osób pozostających na utrzymaniu i świadczeń, szkolenia, prowadzenie akt Pracowników, sprawy dyscyplinarne i rozwiązywanie umów, ustalenia dotyczące podróży, zapewnianie właściwego bezpieczeństwa i inne funkcje administracyjne, które mają na celu pomóc Pracownikom w spełnianiu ich oczekiwań dotyczących pracy.
- IT: zapewnianie właściwego sprzętu i usług IT, obsługa, zarządzanie i ochrona systemów IT i komunikacyjnych Spółki.
- Komunikacja i sytuacje awaryjne: ułatwianie komunikacji z Pracownikami, zapewnianie referencji, ochrona zdrowia i bezpieczeństwa Pracowników i innych osób, ułatwianie komunikacji w celu promowania dobrego samopoczucia Pracowników lub klientów, również w sytuacjach awaryjnych.
- Przestrzeganie zobowiązań prawnych: przestrzeganie naszych zobowiązań regulacyjnych, nakazów sądowych, wezwań sądowych i podobnych żądań;



przeprowadzanie weryfikacji życiorysów zawodowych zgodnie z wymogami obowiązujących przepisów prawa, przeprowadzanie kontroli list wykluczeń i sankcji zgodnie z wymogami obowiązujących przepisów prawa.

- Zgodność z przepisami: prowadzenie i zarządzanie skargami, dochodzeniami i roszczeniami, rozpatrywanie roszczeń związanych z pracą, takich jak pracownicze roszczenia odszkodowawcze, przestrzeganie wymogów prawnych, regulacyjnych i innych, takich jak przepisy BHP, odliczenia od podatku dochodowego i ubezpieczenia społecznego, obowiązki w zakresie prowadzenia dokumentacji i sprawozdawczości, przeprowadzanie audytów, zgodność z inspekcjami rządowymi i innymi żądaniem ze strony rządu, innych organów publicznych lub regulacyjnych, zgodność z wewnętrzną polityką i procedurami, obrona lub wszczynanie postępowań sądowych, odpowiadanie na pozwyc oraz dochodzenie praw i odszkodowań.
- Bezpieczeństwo i ochrona: ochrona bezpieczeństwa innych osób, w tym Pracowników, klientów i ogółu społeczeństwa, a także ochrona własności i aktywów Spółki, takich jak majątek trwały i informacje poufne.
- Inne: realizacja innych celów w ramach naszej działalności biznesowej, gdy jest to przez nas zasadnie wymagane.

Wrażliwe dane osobowe

W niektórych jurysdykcjach, gdzie jest to prawnie dozwolone oraz za zgodą Pracownika, kiedy jest ona wymagana obowiązującymi przepisami prawa, Spółka może przetwarzać pewne kategorie Danych osobowych, które mogą być uważane za wrażliwe w określonych jurysdykcjach („Wrażliwe dane osobowe”), w tym:

- Wydany przez rząd numer identyfikacyjny, taki jak numer ubezpieczenia społecznego, dane z prawa jazdy, dowodu osobistego wydanego przez stan i paszportu.
- Precyzyjne informacje geolokalizacyjne umożliwiające śledzenie lokalizacji pojazdów lub Urządzeń.
- Treść komunikacji, w tym wiadomości e-mail, wiadomości tekstowych i czatów przesyłanych za pomocą Urządzeń używanych do celów służbowych, Urządzeń podłączonych do systemów lub sieci służbowych lub kont zarządzanych przez Spółkę, a także wszelkich innych kont, do których Spółka może mieć uprawniony dostęp. Komunikacja, która jest osobista i niezwiązana z działalnością Spółki, może być potencjalnie dostępna w sposób niezamierzony w ramach przeglądu skoncentrowanego na sprawach Spółki jako informacja dodatkowa lub uzyskana przypadkowo.
- Dane dotyczące wypadków, zdrowia i dane medyczne, status obywatelstwa lub imigracyjny, dane dotyczące rasy lub pochodzenia etnicznego, orientacji seksualnej i tożsamości płciowej w celu wypełniania obowiązków w zakresie zatrudnienia, administrowania świadczeniami, ubezpieczenia, ubezpieczenia społecznego, ułatwienia zakwaterowania, oceny integracji i różnorodności oraz administrowania programami, a także w celu ustalenia lub obrony roszczeń prawnych.
- Dane biometryczne, takie jak skany odcisków palców lub skany twarzy do celów weryfikacji, bezpieczeństwa i kontroli dostępu.

Dane osobowe członków rodziny lub w ramach innych relacji osobistych

Jeśli Pracownik przekazuje Spółce dane osobowe (w tym Wrażliwe dane osobowe) dotyczące beneficjentów, partnerów, członków rodziny lub osób kontaktowych w sytuacjach awaryjnych (zwanych łącznie „Osobami kontaktowymi Pracownika”), obowiązkiem takiego Pracownika jest przekazanie im kopii niniejszej Polityki w celu poinformowania ich o przysługujących im prawach.



Dane osobowe Osoby kontaktowej Pracownika będą przetwarzane wyłącznie w zakresie niezbędnym do administrowania świadczeniami lub komunikowania się z Osobą kontaktową Pracownika w sprawie Pracownika lub w razie potrzeby, na przykład w sytuacjach awaryjnych.

2. JAK PRZECHOWUJEMY DANE OSOBOWE I KTO MA DO NICH DOSTĘP

Spółka przechowuje Dane osobowe w różnych aplikacjach kadrowych i informatycznych, w tym do obsługi listy płac, świadczeń, zarządzania talentami i wydajnością. Spółka może prowadzić osobiste akta osobowe w formie papierowej. Dostęp do Danych osobowych jest ograniczony do osób, które potrzebują takiego dostępu do celów wymienionych powyżej lub gdy jest to wymagane przez prawo, w tym do członków działu zasobów ludzkich, kierowników w obszarze działalności Pracownika oraz do upoważnionych przedstawicieli wewnętrznych funkcji kontrolnych Spółki, takich jak dział księgowości, zgodności z przepisami, prawni i IT. W stosownych przypadkach dostęp może być również udzielany innym Pracownikom Spółki na zasadzie ograniczonego dostępu, na przykład w przypadku, gdy Pracownik jest brany pod uwagę jako kandydat na inne stanowisko lub gdy nowy kierownik w danym obszarze działalności musi przejrzeć akta, lub w związku z dochodzeniami.

3. MIĘDZYKRAJOWE UJAWNIANIE I PRZEKAZYWANIE DANYCH OSOBOWYCH

Spółka może ujawnić Dane osobowe osobom i podmiotom takim jak:

- Dostawcy i usługodawcy, którzy wspierają funkcje związane z zasobami ludzkimi i zgodnością z prawem, w tym w celu weryfikacji zatrudnienia, przeprowadzania kontroli przeszłości, zapewniania szkoleń i przetwarzania roszczeń w miejscu pracy;
- Dostawcy i usługodawcy w celu wsparcia funkcji biznesowych, administracyjnych i zarządczych. Na przykład Spółka może współpracować ze stronami trzecimi w zakresie rekrutacji, IT, konsultacji, doradztwa prawnego, doradztwa zawodowego, audytu, księgowości, komunikacji lub innych celów;
- Administratorzy świadczeń lub usługodawcy w związku z zapewnieniem świadczeń, w tym emerytalnych, zdrowotnych, ubezpieczenia na życie i innych zgodnie z warunkami zatrudnienia;
- Osoby, które Pracownik podaje jako swoje kontakty referencyjne, osoby, które polecily Pracownika na dane stanowisko lub spółki, którym Pracownik podaje firmę Convergent jako kontakt referencyjny;
- Inne spółki zależne i stowarzyszone firmy Convergent;
- Inne spółki w związku z fuzją, sprzedażą, wspólnym przedsięwzięciem, cesją, przeniesieniem lub innym zbyciem całości lub części naszej działalności, aktywów lub akcji (w tym w związku z jakimkolwiek postępowaniem upadłościowym lub podobnym);
- Organy ścigania, bezpieczeństwa lub organy rządowe w celu zapewnienia zgodności z przepisami prawa, regulacjami, nakazami sądowymi, wezwaniami sądowymi i podobnymi żądaniami;
- Partnerzy lub klienci firmy Convergent, na przykład gdy wymagają oni kontroli przeszłości, testów na obecność substancji psychoaktywnych lub innych informacji, aby Pracownik mógł wykonywać dla nich pracę.
- Podmioty lub osoby, które są niezbędne dla ochrony naszych praw, wypełniania naszych zobowiązań prawnych i ochrony zgodnych z prawem interesów pracowników, klientów lub społeczności związanych z bezpieczeństwem;
- Podmioty i osoby, które są niezbędne dla zapewnienia zgodności z obowiązkiem lub żądaniem prawnym, w celu zapewnienia bezpieczeństwa lub innej ochrony praw swoich lub stron trzecich.



4. MIĘDZYNARODOWE PRZEKAZYWANIE DANYCH OSOBOWYCH

Biorąc pod uwagę globalny charakter Spółki, możemy (zgodnie z obowiązującym prawem) przekazywać Dane osobowe innym podmiotom grupy Convergent lub jednostkom stowarzyszonym zlokalizowanym w różnych krajach. Tego typu Dane osobowe mogą być przekazywane w celach określonych powyżej odbiorcom znajdującym się poza jurysdykcją, w której znajduje się Pracownik. Odbiorcy danych mogą znajdować się w krajach, w których przepisy o ochronie danych mogą nie zapewniać poziomu ochrony równego przepisom obowiązującym w jurysdykcji Pracownika. Podmioty należące do grupy Convergent lub jednostki stowarzyszone zawarły wewnątrzgrupową umowę o przekazywaniu danych, która zawiera zobowiązania umowne mające na celu zapewnienie ochrony Danych osobowych podczas przekazywania danych pomiędzy nimi.

W razie potrzeby skorzystamy z odpowiednich mechanizmów transferu, takich jak decyzje o adekwatności lub standardowe klauzule umowne, w przypadku transferów międzynarodowych. Oceniamy lokalne przepisy prawne i w razie potrzeby stosujemy środki uzupełniające.

5. PRAWDŁOWOŚĆ

Dokładamy wszelkich starań, aby zapewnić jak największą dokładność, kompletność i aktualność **danych osobowych** Pracownika. Nie aktualizujemy rutynowo **danych osobowych** Pracowników, chyba że taka aktualizacja jest konieczna. Aby pomóc nam w utrzymaniu i zapewnieniu dokładności oraz aktualności **danych osobowych**, Pracownik powinien niezwłocznie informować nas o wszelkich zmianach w przekazanych nam informacjach.

6. BEZPIECZEŃSTWO

Bezpieczeństwo informacji Pracownika jest dla nas ważne. Spółka stosuje odpowiednie środki administracyjne, techniczne i organizacyjne w celu ochrony przed nieuprawnionym lub niezgodnym z prawem przetwarzaniem Danych osobowych lub przed przypadkową utratą, zmianą, ujawnieniem lub dostępem, a także przypadkowym lub niezgodnym z prawem zniszczeniem lub uszkodzeniem Danych osobowych. Środki te mają na celu promowanie ciągłej integralności i poufności Danych osobowych. Spółka regularnie ocenia takie środki w celu promowania bezpieczeństwa przetwarzania danych.

7. PRZECHOWYWANIE DANYCH

Spółka będzie przechowywać Dane osobowe zgodnie z obowiązującymi wymogami prawnymi i tylko przez taki czas, jaki będzie konieczny do celów opisanych powyżej lub jaki będzie wymagany przez prawo lub w celu obrony potencjalnych roszczeń prawnych. Spółka będzie przechowywać Dane osobowe zgodnie z wszelkimi obowiązującymi, każdorazowo aktualizowanymi zasadami w tym zakresie lub zgodnie z wymogami lub zezwoleniami obowiązującego prawa. W stosownych przypadkach firma Convergent może zanonimizować lub usunąć elementy umożliwiające identyfikację takich Danych osobowych.

8. REZYGNACJA Z OTRZYMYWANIA WIADOMOŚCI TEKSTOWYCH (KANDYDACI Z USA)

Każdorazowo możesz otrzymywać wiadomości tekstowe wysyłane przez firmę Convergent lub w jej imieniu. Kandydaci z USA, którzy nie chcą dalej otrzymywać wiadomości tekstowych od firmy Convergent lub w jej imieniu, mogą wysłać SMS-a z odpowiednim krótkim kodem lub



bezpośrednio odpowiedzieć na dowolną wiadomość otrzymaną od firmy Convergent lub wysłaną w jej imieniu, używając odpowiedniego krótkiego kodu (np. STOP, QUIT, END, REVOKE, OPT OUT, CANCEL lub UNSUBSCRIBE), aby zrezygnować z otrzymywania przyszłych wiadomości tekstowych. Kandydat może otrzymać dodatkową wiadomość SMS potwierdzającą jego decyzję o rezygnacji.

9. DANE KONTAKTOWE

W przypadku jakichkolwiek pytań dotyczących niniejszej Polityki lub w celu skorzystania z obowiązujących praw do prywatności należy skontaktować się z Inspektorem ochrony danych w firmie Convergent pod adresem dataprotectionofficer@convergent.com, przesłać wniosek w zakresie ochrony prywatności danych za pośrednictwem formularza internetowego dostępnego pod adresem <https://www.convergent.com/about/contact-us/>, wpisując „Wniosek w zakresie ochrony prywatności – DW: Dział prawny” w jego treści lub przekazać taki wniosek za pośrednictwem bezpłatnego numeru telefonu: 1-877-641-8181.

10. AKTUALIZACJE POLITYKI

Pracownik może zwrócić się do nas o kopię niniejszej Polityki, korzystając z danych kontaktowych podanych powyżej. Niniejsza Polityka może być okresowo zmieniana według naszego wyłącznego uznania, a wszelkie zmiany wejdą w życie po zaktualizowaniu jej w odpowiednich Regulaminach pracy i w intranecie Spółki. Jeśli wprowadzimy istotne zmiany, powiadomimy o tym Pracownika pocztą elektroniczną na adres e-mail, który mamy zapisany w jego aktach.

ZAŁĄCZNIK I — OCHRONA PRYWATNOŚCI W KALIFORNII

Informacje zawarte w niniejszym Załączniku mają zastosowanie do Pracowników ze stanu Kalifornia. W przypadku jakichkolwiek niezgodności pomiędzy warunkami niniejszego Załącznika a warunkami głównej polityki warunki niniejszego Załącznika mają pierwszeństwo. Jako mieszkaniec stanu Kalifornia Pracownik może składać następujące wnioski dotyczące swoich danych osobowych zgodnie z obowiązującym prawem:

- **Wniosek o dostęp** – informacje na temat kategorii Danych osobowych; kategorii źródeł tych Danych osobowych; celów biznesowych lub handlowych, dla których gromadzimy Dane osobowe; oraz stron trzecich, którym ujawniamy Dane osobowe, zostały ujawnione w sekcjach 1 i 3 niniejszej Polityki. Pracownik może zażądać, abyśmy ujawnili mu w przenośnym formacie kategorie gromadzonych na jego temat Danych osobowych, kategorie źródeł, z których gromadzone są Dane osobowe, kategorie sprzedawanych lub ujawnianych Danych osobowych, biznesowy lub komercyjny cel gromadzenia Danych osobowych, kategorie stron trzecich, którym ujawniamy Dane osobowe, oraz konkretne fragmenty Danych osobowych zgromadzonych na temat Pracownika w ciągu co najmniej ostatnich 12 miesięcy;
- **Wniosek o usunięcie danych** – Pracownik może zażądać od nas usunięcia jego Danych osobowych, które przechowujemy na jego temat, z zastrzeżeniem pewnych wyjątków. Usuniemy z naszych rejestrów lub zanonimizujemy Dane osobowe, które nie podlegają zgodnemu z prawem wyłączeniu. Należy pamiętać, że prawo przewiduje szereg wyjątków, na podstawie których nie jesteśmy zobowiązani lub możemy nie być w stanie usunąć Danych osobowych Pracownika.
- **Wniosek o sprostowanie** – Pracownik może zażądać od nas sprostowania jego Danych osobowych, na przykład gdy są nieprawidłowe, niekompletne lub nieaktualne.



- **Wniosek o ograniczenie wykorzystania / ujawniania Wrażliwych danych osobowych** – Pracownik może zażądać, abyśmy ograniczyli wykorzystanie lub ujawnienie jego Wrażliwych danych osobowych do celów niezgodnych z ujawnionym celem, dla którego Wrażliwe dane osobowe zostały zgromadzone, z zastrzeżeniem pewnych wyjątków. Wykorzystujemy Wrażliwe Dane osobowe wyłącznie w zakresie niezbędnym do świadczenia usług, dla których zostały zebrane, zgodnie z powyższym opisem.
- **Wniosek o rezygnację ze sprzedaży lub udostępniania** – Nie sprzedajemy ani nie udostępniamy Danych osobowych Pracowników zgodnie z definicjami tych terminów zawartymi w prawie stanu Kalifornia. W ciągu ostatnich 12 miesięcy nie sprzedaliśmy ani nie udostępniliśmy żadnych Danych osobowych stronom trzecim. Dla celów niniejszej sekcji „sprzedaż” oznacza sprzedaż, wynajem, wydanie, ujawnianie, rozpowszechnianie, udostępnianie, przekazanie lub inne ustne, pisemne lub elektroniczne przekazanie Danych osobowych Pracownika podmiotowi zewnętrznemu za wynagrodzeniem pieniężnym lub innym, a „udostępnianie” oznacza ujawnienie Danych osobowych podmiotom zewnętrznym do celów przekrojowej reklamy behawioralnej, z zastrzeżeniem pewnych wyjątków przewidzianych w obowiązującym prawie.

Aby skorzystać z powyższych praw, Pracownik powinien złożyć wniosek, korzystając z metod kontaktu podanych poniżej. W zależności od wniosku Pracownika możemy zażądać od niego pewnych informacji w celu zweryfikowania jego tożsamości i miejsca zamieszkania. Etapy weryfikacji będą się różnić w zależności od wrażliwości Danych osobowych.

Możemy odrzucić niektóre wnioski lub spełnić je tylko częściowo, w oparciu o nasze prawa i obowiązki. Możemy na przykład przechowywać Dane osobowe w zakresie dozwolonym przez prawo, np. do celów podatkowych, zasiłków dla bezrobotnych lub innych celów ewidencyjnych, w celu administrowania świadczeniami lub w ramach toczącego się postępowania sądowego. Spółka nie będzie dyskryminować Pracowników ani stosować wobec nich żadnych form odwetu za korzystanie z praw przysługujących im na mocy niniejszej sekcji.

Mieszkańcy stanu Kalifornia mogą wyznaczyć upoważnionego przedstawiciela do złożenia wniosku w ich imieniu. Przesyłając wniosek, należy upewnić się, że upoważniony przedstawiciel został jako taki zidentyfikowany i że posiada informacje niezbędne do ukończenia procesu weryfikacji. W zależności od wrażliwości Danych osobowych w przypadku korzystania z autoryzowanego przedstawiciela może być konieczne zweryfikowanie autentyczności wniosku bezpośrednio z Pracownikiem.

ZAŁĄCZNIK II: OCHRONA PRYWATNOŚCI W KANADZIE

Informacje zawarte w niniejszym Załączniku mają zastosowanie do Pracowników z Kanady. W przypadku jakichkolwiek niezgodności pomiędzy warunkami niniejszego Załącznika a warunkami głównej polityki warunki niniejszego Załącznika mają pierwszeństwo. W zależności od prowincji kanadyjskiej, w której mieszka Pracownik, może on mieć następujące prawa w odniesieniu do wykorzystywania przez nas jego Danych osobowych:

- **Dostęp i mobilność** — użytkownik może mieć prawo do złożenia wniosku o udzielenie informacji, czy przechowujemy jego Dane osobowe, oraz do uzyskania kopii takich informacji. W tym celu prosimy o kontakt pod adresem: dataprotectionofficer@convergent.com. Istnieją wyjątki od tego prawa, więc możemy odmówić dostępu, jeśli na przykład udostępnienie informacji Pracownikowi spowodowałoby ujawnienie Danych osobowych innej osoby lub jeśli przepisy prawa zabraniają nam ujawniania takich informacji. Pracownik może również mieć prawo do żądania, aby zebrane od niego cyfrowe Dane osobowe zostały przekazane



w powszechnie stosowanym formacie technologicznym temu, a także każdej osobie lub organowi upoważnionemu przez prawo do gromadzenia takich informacji. Prawo to nie obejmuje informacji, które zostały utworzone lub wywnioskowane na podstawie Danych osobowych Pracownika, a my nie mamy obowiązku przekazywania takich informacji, jeśli wiąże się to z poważnymi trudnościami praktycznymi.

- **Prawo do prawidłowości danych** – dążymy do tego, aby Dane osobowe Pracownika były prawidłowe, aktualne i kompletne. Zachęcamy do kontaktu z nami pod adresem dataprotectionofficer@convergint.com, aby poinformować nas o wszelkich nieścisłościach lub zmianach dotyczących Danych osobowych, tak abyśmy mogli je zaktualizować.
- **Prawo do wycofania zgody** – jeśli Pracownik wyraził zgodę na przetwarzanie jego Danych osobowych, może mieć prawo do całkowitego lub częściowego wycofania swojej zgody. W celu wycofania zgody prosimy o kontakt pod adresem: dataprotectionofficer@convergint.com. Po otrzymaniu powiadomienia o wycofaniu zgody przez Pracownika nie będziemy już przetwarzać jego danych w celach, na które pierwotnie wyraził zgodę, chyba że istnieje inna podstawa prawna przetwarzania.
- **Zaprzestanie rozpowszechniania i usunięcie z indeksu** – Pracownik może mieć prawo do żądania zaprzestania rozpowszechniania swoich danych osobowych i/lub usunięcia z indeksu wszelkich hiperłączy powiązanych z jego imieniem i nazwiskiem, jeśli takie działania są sprzeczne z prawem lub nakazem sądowym lub jeśli spełnione są następujące warunki:
 - rozpowszechnianie informacji wyrządza Pracownikowi poważną szkodę w odniesieniu do jego prawa do poszanowania reputacji lub prywatności;
 - szkoda jest wyraźnie większa niż interes publiczny w poznaniu informacji lub interes prawny jakiegokolwiek osoby do swobodnego wyrażania opinii; oraz
 - żądane zaprzestanie rozpowszechniania nie wykracza poza działania konieczne do zapobieżenia utrwaleniu się szkody.
- **Prawo do ponownej indeksacji** – Pracownik może mieć prawo zażądać ponownej indeksacji łącza zapewniającego dostęp do informacji, jeśli spełnione są następujące warunki:
 - niedopełnienie tego obowiązku spowoduje poważną szkodę w odniesieniu do prawa Pracownika do poszanowania jego reputacji lub prywatności;
 - szkoda spowodowana brakiem ponownej indeksacji jest większa niż interes publiczny w poznaniu informacji lub interes prawny jakiegokolwiek osoby do swobodnego wyrażania opinii; oraz
 - żądana ponowna indeksacja nie wykracza poza działania konieczne do zapobieżenia utrwaleniu się szkody.
- **Prawo do zaskarżenia** – jeśli Pracownik uważa, że jego prawa do ochrony Danych osobowych zostały naruszone, ma prawo złożyć skargę do właściwego organu nadzorczego lub dochodzić zadośćuczynienia na drodze sądowej.

Pracownik może zapytać o swoje Dane osobowe, kontaktując się z nami pod adresem dataprotectionofficer@convergint.com. Co do zasady odpowiemy na wszystkie wnioski o dostęp w ciągu 30 dni od otrzymania wszelkich niezbędnych informacji. W okolicznościach, w których nie będziemy w stanie zapewnić dostępu lub jeśli spełnienie wniosku będzie wymagało dodatkowego czasu, informujemy o tym Pracownika na piśmie. Możemy nie ujawniać pewnych rodzajów informacji na podstawie wyłączeń określonych w obowiązujących przepisach prawa. Gdy to możliwe, oddzielimy informacje, które nie zostaną ujawnione i zapewnimy Pracownikowi dostęp do pozostałych informacji. Jeśli nie będziemy w stanie zapewnić Pracownikowi dostępu do Danych osobowych lub ich ujawnić, prześlemy mu wyjaśnienie, z zastrzeżeniem ograniczeń. W pewnych okolicznościach, np. gdy wniosek będzie nadmierny lub nieuzasadniony, możemy obciążyć Pracownika opłatą administracyjną za dostęp do jego Danych osobowych. Możemy również pobierać opłaty za dodatkowe kopie. Poinformujemy Pracownika o wszelkich opłatach przed przystąpieniem do realizacji wniosku.

ZAŁĄCZNIK III: OCHRONA PRYWATNOŚCI W EUROPIE

Informacje zawarte w niniejszym Załączniku mają zastosowanie do Pracowników z Wielkiej Brytanii, Europejskiego Obszaru Gospodarczego lub Szwajcarii. W przypadku jakichkolwiek niezgodności pomiędzy warunkami niniejszego Załącznika a warunkami głównej polityki warunki niniejszego Załącznika mają pierwszeństwo.

1. PODSTAWA PRAWNA

Zgodnie z określonymi przepisami prawa dotyczącymi prywatności, w tym RODO, musimy mieć podstawę prawną do przetwarzania Danych osobowych Pracownika. Jak opisano powyżej, Spółka wykorzystuje Dane osobowe Pracownika z następujących prawnie uzasadnionych powodów:

- **Uzasadnione cele biznesowe:** gdy mamy uzasadniony interes biznesowy w przetwarzaniu Danych osobowych Pracownika, pod warunkiem, że jego interesy i podstawowe prawa nie są nadrzędne wobec tych interesów.
- **Umowne:** przetwarzamy Dane osobowe Pracownika przede wszystkim w celu realizacji umów, w tym w zakresie wynagrodzeń, wdrażania nowych pracowników i ocen wyników pracy.
- **Zobowiązania prawne:** istnieje prawny lub regulacyjny obowiązek przetwarzania Danych osobowych Pracownika i musimy go przestrzegać.
- **Zgoda:** w ograniczonych okolicznościach możemy poprosić Pracownika o wyrażenie zgody na przetwarzanie przez nas jego Danych osobowych, a w przypadku wyrażenia takiej zgody Pracownik ma prawo wycofać ją w dowolnym momencie. Dodatkowe informacje na temat tego, jakiego przetwarzania danych dotyczy ta zgoda, zostaną przekazane Pracownikowi w momencie, gdy poprosimy go o wyrażenie zgody.

Nie podejmujemy decyzji mających skutki prawne lub podobne znaczenie wyłącznie w oparciu o automatyzację.

Jak wyjaśniono w innym przepisie niniejszej Polityki, dane wrażliwe podlegają bardziej restrykcyjnym wymogom. Możemy przetwarzać dane wrażliwe w następujących okolicznościach:

- w ograniczonych sytuacjach, za wyraźną pisemną zgodą Pracownika;
- w przypadku, gdy musimy wypełniać nasze zobowiązania prawne lub korzystać z praw związanych z zatrudnieniem, np. w odniesieniu do Pracowników niepełnosprawnych;
- gdy jest to konieczne w interesie publicznym, np. w celu monitorowania równości szans lub w związku z naszym pracowniczym programem emerytalnym;
- gdy jest to konieczne w celu ochrony Pracownika lub innej osoby przed szkodą;
- gdy są one potrzebne w związku z roszczeniami prawnymi lub gdy są one potrzebne do ochrony interesów Pracownika (lub interesów innej osoby), a Pracownik nie jest w stanie wyrazić na to zgody lub gdy Pracownik już upublicznił te informacje.

2. PRAWA

Pracownik ma pewne prawa wynikające z europejskich przepisów o ochronie danych. Zostały one określone poniżej. Należy jednak pamiętać, że nie są to prawa bezwzględne i istnieją ich ograniczenia, a niektóre z nich mogą nie być dostępne dla Pracownika w odniesieniu do wszystkich Danych osobowych.

- **Prawo do informacji** – Pracownik ma prawo do otrzymania jasnych, przejrzystych



i zrozumiałych informacji o tym, w jaki sposób wykorzystujemy jego dane oraz o przysługujących mu prawach. Dlatego też przekazujemy Pracownikowi informacje zawarte w niniejszej Polityce.

- **Prawo do dostępu** – Pracownik ma prawo do uzyskania dostępu do swoich danych (jeśli je przetwarzamy) i niektórych innych informacji (podobnych do tych podanych w niniejszej Polityce). Dzięki temu Pracownik jest świadomy i może sprawdzić, czy wykorzystujemy jego dane zgodnie z przepisami o ich ochronie.
- **Prawo do usunięcia** – znane również jako „prawo do bycia zapomnianym”. Mówiąc prościej, umożliwia ono Pracownikowi zażądania usunięcia jego Danych osobowych, jeśli nie ma istotnego powodu, abyśmy nadal z nich korzystali. Nie jest to ogólne prawo do usunięcia danych; istnieją wyjątki.
- **Prawo do sprostowania** – Pracownik ma prawo do sprostowania swoich danych, jeśli są one niedokładne lub niekompletne.
- **Prawo do zgody** – jeśli Pracownik wyraził zgodę na przetwarzanie danych, ma prawo do jej wycofania. Jak jednak wyjaśniono w sekcji 3 powyżej, zasadniczo nie opieramy się na zgodzie jako zgodnej z prawem podstawie przetwarzania.
- **Prawo do ograniczenia** – Pracownik ma prawo ograniczyć przetwarzanie swoich danych osobowych, co oznacza, że może poprosić nas o ograniczenie tego, co z nimi robimy.
- **Prawo do sprzeciwu** – Pracownik ma prawo sprzeciwić się niektórym rodzajom przetwarzania, w tym przetwarzaniu w oparciu o nasze uzasadnione interesy w niektórych przypadkach.
- **Prawo do przenoszenia** – Pracownik ma prawo do uzyskania i ponownego wykorzystania swoich danych osobowych do własnych celów w ramach różnych usług.
- **Prawo do skargi** – Pracownik może złożyć skargę do lokalnego organu nadzorczego, jak opisano poniżej. Pracownicy mieszkający w Wielkiej Brytanii zgodnie z lokalnymi przepisami mają dodatkowe prawo do złożenia skargi bezpośrednio do nas, korzystając z poniższego adresu e-mail.

Aby złożyć taki wniosek lub sprzeciw, należy wysłać wiadomość e-mail na adres dataprotectionofficer@convergint.com.

Pracownik może być również uprawniony do złożenia skargi do właściwego organu ochrony danych. Nazwy i dane kontaktowe organów ochrony danych w Unii Europejskiej można znaleźć na stronie http://ec.europa.eu/justice/article-29/structure/data-protection-authorities/index_en.htm. Organem ochrony danych w Wielkiej Brytanii jest Information Commissioner's Office, a jego dane kontaktowe można znaleźć na stronie <https://ico.org.uk/global/contact-us/>. Szwajcarskim organem jest FDPIC, a jego dane kontaktowe można znaleźć na stronie <https://www.edoeb.admin.ch/edoeb/en/home.html>.

ZAŁĄCZNIK IV: OCHRONA PRYWATNOŚCI W AZJI

Jeśli Pracownik przebywa poza Chinami i Indiami, prosimy o kontakt pod adresem dataprotectionofficer@convergint.com, aby dowiedzieć się więcej o prawach dotyczących prywatności, które mogą mu przysługiwać.

Mieszkańcy Chin i Indii znajdą w tej sekcji informacje o podstawach prawnych, w oparciu o które przetwarzamy ich Dane osobowe, jak również prawa dotyczące prywatności, informacje o Wrażliwych danych osobowych i Transgranicznym przekazywaniu danych zgodnie z obowiązującymi przepisami prawa, w tym Prawem ochrony danych osobowych ChRL (PIPL),



Ustawą o ochronie cyfrowych danych osobowych w Indiach, Ustawą DPDP z 2023 r. oraz wydanych zgodnie z nimi zasadami i regulacjami. W przypadku jakichkolwiek niezgodności pomiędzy warunkami niniejszego Załącznika a pozostałą częścią Polityki warunki niniejszego Załącznika będą mieć pierwszeństwo.

1. PODSTAWA PRAWNA

Chiny	Indie
<p>Zbieramy i wykorzystujemy Dane osobowe Pracownika tylko wtedy, gdy jest to konieczne do celów wskazanych wyżej w niniejszej Polityce. W zależności od okoliczności możemy opierać się na jednej lub kilku z poniższych podstaw prawnych:</p> <ul style="list-style-type: none"> • Zgoda Pracownika – w przypadku gdy uzyskamy zgodę Pracownika. • Zarządzanie zasobami ludzkimi – w przypadku gdy jest to niezbędne do wdrożenia zarządzania zasobami ludzkimi zgodnie z niniejszą polityką i innymi regulaminami zatrudnienia. • Wymogi prawne – w przypadku gdy jest to niezbędne do wykonania obowiązków prawnych lub spełnienia wymogów prawnych. • Sytuacje kryzysowe – w przypadku gdy jest to niezbędne w celu udzielenia odpowiedzi służbom publicznej ochrony zdrowia lub w celu ochrony życia, zdrowia i bezpieczeństwa mienia w sytuacji kryzysowej. • Dane osobowe ujawnione przez Pracownika – w przypadku, gdy Pracownik ujawnił swoje Dane osobowe lub Dane osobowe Pracownika zostały ujawnione publicznie. • Inne podstawy prawne określone w ustawie PIPL i innych stosownych przepisach prawa i regulacjach Chińskiej Republiki Ludowej. 	<p>Przetwarzamy Dane osobowe Pracownika wyłącznie w sposób zgodny z obowiązującymi przepisami prawa i regulacjami, do celów zgodnych z prawem:</p> <ul style="list-style-type: none"> • na które Pracownik wyraził zgodę; lub • do pewnych zgodnych z prawem zastosowań, w tym: <ul style="list-style-type: none"> – do określonych celów, do których Pracownik dobrowolnie przekazał nam swoje Dane osobowe i w stosunku do których Pracownik nie wskazał nam, że nie wyraża zgody na wykorzystywanie jego Danych osobowych; – do celów zatrudnienia lub związanych z zabezpieczeniem nas przed stratą lub odpowiedzialnością, takich jak zapobieganie szpiegostwu gospodarczemu, zachowanie poufności tajemnic handlowych, własności intelektualnej, informacji tajnych lub świadczenia wszelkich usług lub świadczeń, których dochodzi pracownik; lub – w celu spełnienia obowiązku prawnego lub regulacyjnego.

2. WRAŻLIWE DANE OSOBOWE

Możemy przetwarzać Wrażliwe dane osobowe Pracownika wymienione powyżej. Jeśli jest to wymagane obowiązującymi przepisami prawa i regulacjami, uzyskamy osobną zgodę Pracownika. Dla jasności, niektóre przepisy (takie jak ustawa DPDP) nie regulują kwestii Wrażliwych danych osobowych jako odrębnej kategorii ustawowej.

3. TRANSGRANICZNE PRZEKAZYWANIE DANYCH

W celu prowadzenia działań w zakresie globalnego zarządzania zasobami ludzkimi, globalnych projektów i administracji gospodarczej grupa Convergent lub jednostki stowarzyszone korzystają z ujednoczonych lub wewnętrznie połączonych systemów informatycznych do przetwarzania Danych osobowych Pracownika. Przekazywanie Danych osobowych Kontrahenta poza Chiny lub Indie do spółek grupy Convergent lub jednostek stowarzyszonych zlokalizowanych w innym miejscu jest więc niezbędne dla Spółki. Jeśli jest to wymagane obowiązującymi przepisami prawa i regulacjami, wdrożymy właściwe mechanizmy dla transgranicznego przekazywania danych i przeprowadzimy właściwe procedury. Będziemy powiadamiać Pracownika o wszystkich istotnych informacjach związanych z przekazywaniem danych za granicę i uzyskamy jego osobną zgodę, jeśli będą wymagać tego obowiązujące przepisy prawa i regulacje.

4. PRAWA

Chiny	Indie
<p>Pracownik posiada pewne prawa wynikające z Ustawy o ochronie Danych osobowych Chińskiej Republiki Ludowej („PIPL”) i innych obowiązujących w Chinach przepisów prawa i regulacji. Zostały one określone poniżej:</p> <ul style="list-style-type: none"> • Prawo do informacji – Pracownik ma prawo do informacji i podejmowania decyzji dotyczących przetwarzania jego Danych osobowych. • Prawo do odmowy – Pracownik ma prawo do ograniczenia lub odmówienia innym zgody na przetwarzanie jego Danych osobowych. • Prawo do dostępu – Pracownik ma prawo do wglądu do jego Danych osobowych lub uzyskania ich kopii. • Prawo do przeniesienia – Pracownik ma prawo żądać od nas przeniesienia jego Danych osobowych do strony trzeciej przez niego wyznaczonej, w zakresie dozwolonym przez obowiązujące przepisy prawa i regulacje. • Prawo do korekty – Pracownik ma prawo żądać od nas wprowadzenia korekty lub uzupełnienia, jeśli dowie się, że jego Dane osobowe są niepoprawne lub niekompletne. • Prawo do usunięcia – Pracownik ma prawo do usunięcia swoich Danych osobowych, które nam przekazał, jednak w przypadku gdy okres przechowywania wyznaczony przez obowiązujące przepisy prawa i regulacje jeszcze nie upłynął lub gdy usunięcie Danych osobowych sprawia techniczną trudność, zakończymy przetwarzanie tych Danych osobowych za wyjątkiem ich przechowywania 	<p>Pracownik posiada pewne prawa wynikające z Ustawy o ochronie cyfrowych danych osobowych („Ustawa DPDP”) i innych obowiązujących w Indiach przepisów prawa i regulacji. Zostały one określone poniżej:</p> <ul style="list-style-type: none"> • Prawo dostępu do informacji o Danych osobowych – w zakresie dozwolonym przez obowiązujące przepisy prawa i regulacje Pracownik ma prawo żądać od nas podsumowania przetwarzanych przez nas Danych osobowych, ujawnienia tożsamości innych powierników danych i podmiotów przetwarzających dane, którym udostępniłmy jego Dane osobowe, opisu jego Danych osobowych udostępnionych stronom trzecim, a także wszelkich innych informacji związanych z jego Danymi osobowymi, pod warunkiem, że udzielił nam zgody na przetwarzanie takich Danych osobowych. • Prawo do korekty i usunięcia Danych osobowych – Pracownik ma prawo do korekty, uzupełnienia, zaktualizowania i usunięcia swoich Danych osobowych, co do których wyraził wcześniej zgodę na ich przetwarzanie. • Prawo do wycofania zgody – Pracownik ma prawo do wycofania swojej zgody na przetwarzanie jego Danych osobowych w dowolnym czasie po udzieleniu takiej zgody. • Prawo do dochodzenia roszczeń – Pracownik ma prawo uzyskać od nas łatwo dostępne środki dochodzenia roszczeń w przypadku jakiegokolwiek zaniechania dopuszczonego się przez nas w stosunku do

<p>i stosowania niezbędnych środków ochrony ich bezpieczeństwa.</p> <ul style="list-style-type: none"> • Prawo do wyjaśnienia – Pracownik ma prawo żądać od nas wyjaśnienia zasad, według których przetwarzamy Dane osobowe. 	<p>wykonania naszych obowiązków związanych z jego Danymi osobowymi lub wykonania jego praw. Jeśli Pracownik nie jest zadowolony z naszej odpowiedzi na swoją skargę, może zgodnie z obowiązującym prawem skierować ją do Indyjskiej Komisji Ochrony Danych.</p> <ul style="list-style-type: none"> • Prawo wskazania następcy – Pracownik ma prawo wskazać dowolną osobę fizyczną, która, w razie jego śmierci lub ubezwłasnowolnienia, będzie wykonywać prawa związane z danymi Pracownika.
--	--

ZAŁĄCZNIK V: OCEANIA

Jeśli Pracownik przebywa poza Australią i Nową Zelandią, prosimy o kontakt pod adresem dataprotectionofficer@convergint.com, aby dowiedzieć się więcej o prawach dotyczących prywatności, które mogą mu przysługiwać.

Mieszkańcy Australii i Nowej Zelandii mają prawo zażądać dostępu do swoich danych osobowych przechowywanych przez firmę Convergent lub ich poprawienia, a także złożyć skargę dotyczącą sposobu, w jaki przetwarzamy Dane osobowe. Aby uzyskać dostęp do swoich danych osobowych lub złożyć skargę, prosimy o wysłanie wiadomości e-mail na adres:

dataprotectionofficer@convergint.com, podając swoje imię i nazwisko oraz dane kontaktowe oraz wyjaśniając swoją prośbę lub skargę. Firma Convergent doloży starań, aby odpowiedzieć na wiadomość w ciągu 30 dni kalendarzowych od otrzymania wniosku. Firma Convergent może odmówić realizacji wniosku w określonych okolicznościach zgodnie z obowiązującymi przepisami prawa, na przykład jeśli między spółką Convergent a wnioskodawcą lub inną określoną stroną trzecią toczy się lub przygotowywane jest postępowanie sądowe.

Dane osobowe mogą być ujawniane powiązanim podmiotom firmy Convergent oraz dostawcom usług zlokalizowanym za granicą. W takich przypadkach firma Convergent podejmuje uzasadnione kroki w celu zapewnienia, że odbiorcy zagraniczni przetwarzają Dane osobowe zgodnie z obowiązującymi przepisami dotyczącymi ochrony prywatności.

Mieszkańcy Australii, którzy nie są zadowoleni z odpowiedzi udzielonej przez firmę Convergent, mogą złożyć skargę w Office of the Australian Information Commissioner (OAIC), dzwoniąc na numer 1300 363 992 lub korzystając ze strony internetowej OAIC pod adresem <https://www.oaic.gov.au/>. Mieszkańcy Nowej Zelandii powinni kontaktować się z New Zealand Privacy Commissioner przez stronę internetową pod adresem <https://www.privacy.org.nz/your-rights/making-a-complaint-to-the-privacy-commissioner/>.

ZAŁĄCZNIK VI: KRAJE AMERYKI ŁACIŃSKIEJ

ARGENTYNA

Jeśli jesteś mieszkańcem Argentyny, przysługują Ci określone prawa wynikające z ustawy o ochronie danych osobowych nr 25.326 („PDPL”), rozporządzenia wykonawczego nr 1558/2001, dodatkowych zasad i przepisów wydanych przez argentyński organ ochrony danych, zgodnie z poniższym opisem. Niniejsza sekcja dotyczy zarówno osób fizycznych, jak i prawnych, których dane są przetwarzane.



Administrator danych. Administratorem danych odpowiedzialnym za przetwarzanie danych osobowych użytkownika jest firma Seal Solucion de Integracion SRL z siedzibą w Argentynie.

Dostarczanie Danych osobowych. Dostarczanie Danych osobowych jest dobrowolne, jednak niepodanie niektórych informacji lub podanie fałszywych lub niedokładnych informacji może utrudnić nam wykonywanie praw i obowiązków niezbędnych do utrzymania stosunku pracy z Pracownikiem lub uniemożliwić Pracownikowi wykonywanie przysługujących mu praw ustawowych.

Podstawa prawna: Zgodnie z PDPL musimy mieć podstawę prawną do przetwarzania Danych osobowych Pracownika. W zależności od okoliczności możemy opierać się na jednej lub kilku z poniższych podstaw prawnych:

- **Zgoda Pracownika** – w przypadku uzyskania uprzedniej, wyraźnej i świadomej zgody Pracownika. Poprzez zapoznanie się z niniejszą Polityką i uznanie jej zapisów, Pracownik niniejszym udziela zgody na przetwarzanie przez nas jego Danych osobowych zgodnie z niniejszą Polityką.
- **Źródła publicznie dostępne bez ograniczeń** – dane osobowe Pracownika są pozyskiwane z publicznie dostępnych źródeł.
- **Obowiązek prawny** – w przypadku konieczności dostosowania się do obowiązujących uprawnień rządowych lub na mocy obowiązku prawnego.
- **Podstawowe dane identyfikacyjne** – gdzie Dane osobowe Pracownika obejmują wyłącznie imię i nazwisko, dokument tożsamości, numer identyfikacji podatkowej lub emerytalnej, zawód, datę urodzenia i miejsce zamieszkania.
- **Relacja umowna** – gdy Dane osobowe Pracownika wynikają z relacji umownej, naukowej lub zawodowej z Pracownikiem i są niezbędne do rozwoju lub realizacji takiej relacji.

Międzynarodowe przekazywanie danych: W przypadku konieczności przekazania Danych osobowych Pracownika stronom trzecim znajdującym się poza terytorium Argentyny należy pamiętać, że kraje te mogą nie zapewniać poziomu ochrony danych osobowych równoważnego z poziomem zapewnianym przez argentyńską ustawę PDPL. Akceptując niniejszą Politykę prywatności, Kontrahent wyraża wyraźną zgodę na takie międzynarodowe przekazywanie danych, jeśli będzie to konieczne.

Prawa osób, których dane dotyczą: Jeśli Pracownik jest mieszkańcem Argentyny, zgodnie z PDPL przysługują mu następujące prawa:

- **Informacje** – przed zebraniem danych Pracownika ma on prawo do uzyskania informacji o celu przetwarzania i jego odbiorcach, istnieniu bazy danych, tożsamości i siedzibie administratora danych, o tym, czy podanie informacji jest obowiązkowe czy dobrowolne, oraz o konsekwencjach podania lub odmowy podania swoich danych.
- **Dostęp** – Pracownik ma prawo uzyskać dostęp do swoich danych osobowych w ciągu dziesięciu (10) dni kalendarzowych od złożenia wniosku.
- **Poprawianie, aktualizowanie i usuwanie danych** – Pracownik ma prawo zażądać



poprawienia, aktualizacji lub usunięcia swoich danych osobowych, jeśli są one nieprawidłowe, niekompletne, nieaktualne lub nie są już potrzebne do celów, dla których zostały zebrane. Administrator danych musi podjąć działania w ciągu pięciu (5) dni roboczych od otrzymania wniosku. Usunięcie nie nastąpi, jeżeli może to naruszyć prawa lub uzasadnione interesy stron trzecich lub jeżeli istnieje prawny obowiązek zachowania danych.

- **Poufność** – Pracownik ma prawo zażądać, aby jego dane osobowe były traktowane jako poufne.
- **Skargi** – AGENCJA DS. DOSTĘPU DO INFORMACJI PUBLICZNYCH, pełniąca funkcję organu kontrolnego PDPL, jest uprawniona do rozpatrywania skarg i wniosków składanych przez osoby, których prawa zostały naruszone w wyniku nieprzestrzegania obowiązujących przepisów dotyczących ochrony danych osobowych.

Aby skorzystać ze swoich praw, prosimy o wysłanie wiadomości e-mail na adres dataprotectionofficer@convergint.com, określając swoją prośbę i podając szczegóły umożliwiające weryfikację tożsamości.

CHILE

Poniższe informacje dotyczą mieszkańców Chile. Firma Convergint Chile Servicios de Integración SpA, RUT 76.962.871-1, reprezentowana przez Andreę Gutiérrez Rojas, posiadającą dowód osobisty nr 12.722.406-4, zamieszkałą w mieście Santiago, Las Condes, Cerro El Plomo 5855, biuro 307, przetwarza dane osobowe Pracownika zgodnie z ustawą nr 19.628 o ochronie życia prywatnego i jej zmianami wprowadzonymi ustawą nr 21.719 o ochronie danych osobowych (razem „Ustawa o ochronie danych osobowych” lub „LPDP”), konstytucją polityczną Chile i innymi obowiązującymi przepisami.

W okresie prawnej próżni przed pełnym wejściem w życie ustawy nr 21.719 firma Convergint będzie stosować standardy wprowadzone przez tę ustawę w najszerszym możliwym zakresie, zgodnie z systemem wdrożeniowym ustanowionym przez chilijskie przepisy.

Podstawa prawna przetwarzania danych:

Zgodnie z LPDP przetwarzanie danych osobowych musi być uzasadnione na podstawie prawnej uznanej przez prawo. W zależności od danej operacji przetwarzania danych firma Convergint może powołać się na następujące podstawy prawne:

- **Zgoda:** Po wyrażeniu przez Pracownika dobrowolnej, świadomej, konkretnej i jednoznacznej zgody na przetwarzanie jego Danych osobowych w jednym lub kilku określonych celach. W przypadku, gdy przetwarzanie danych opiera się na zgodzie Pracownika, ma on prawo ją cofnąć w dowolnym momencie, bez wpływu na zgodność z prawem przetwarzania danych przed cofnięciem zgody (art. 12 LPDP).
- **Wykonanie lub realizacja umowy:** Gdy przetwarzanie jest niezbędne do wykonania umowy, której stroną jest Pracownik lub do podjęcia działań przed zawarciem umowy na żądanie Kontrahenta (art. 13 lit. c) LPDP).
- **Wypełnienie obowiązku prawnego:** Gdy przetwarzanie jest niezbędne do wypełnienia



obowiązku prawnego lub regulacyjnego mającego zastosowanie do firmy Convergent (art. 13 b) LPDP).

- **Konieczność przetwarzania danych do celów profilaktyki lub medycyny pracy, oceny zdolności kandydata do pracy, diagnozy medycznej, świadczenia opieki zdrowotnej lub społecznej, lub leczenia, lub zarządzania systemami i usługami opieki zdrowotnej lub społecznej:** W celu określenia zdolności kandydata do pracy i podjęcia świadomej decyzji podczas procesu rekrutacyjnego będziemy przetwarzać jego dane dotyczące zdrowia. Obejmuje to wyniki badań lekarskich oraz oceny psychologiczne, psychospołeczne lub psychometryczne, zgodnie z wymaganiami. Przetwarzanie tych danych osobowych jest uzasadnione celami medycyny pracy oraz oceną zdolności do pracy kandydata (art. 16 bis e LPDP).
- **W celu ochrony życia, integralności fizycznej lub zdrowia psychicznego osoby, której dane dotyczą, lub innej osoby; lub gdy osoba, której dane dotyczą, nie jest fizycznie lub prawnie zdolna do wyrażenia zgody:** Na przykład w przypadku kryzysu zdrowotnego dotyczącego współpracownika o tak dużym nasileniu, że nie jest możliwe uzyskanie jego zgody, w celu przewiezienia go do najbliższego ośrodka opieki medycznej (art. 16 bis a LPDP).
- **Uzasadnione interesy:** Gdy przetwarzanie jest niezbędne do realizacji uzasadnionych interesów firmy Convergent lub strony trzeciej, pod warunkiem że nie wpływa to na prawa i wolności osoby, której dane dotyczą. W przypadku powołania się na tę podstawę firma Convergent musi przeprowadzić odpowiednią ocenę proporcjonalności, a Pracownik może w dowolnym momencie zażądać informacji dotyczących uzasadnionego interesu, który ją uzasadnia (art. 13 lit. d) LPDP). Podstawa ta będzie w pełni dostępna po wejściu w życie ustawy nr 21.719.
- **Formułowanie, egzekwowanie lub obrona praw w sądzie:** Gdy przetwarzanie jest niezbędne do formułowania, egzekwowania lub obrony roszczeń przed sądami lub organami publicznymi (art. 13 e) LPDP).

Przetwarzane Dane osobowe, źródła, z których je pozyskujemy, nasze działania związane z przetwarzaniem danych i cele, transfery danych, środki ochrony danych oraz praktyki dotyczące przechowywania danych zostały opisane w głównej części niniejszej Polityki powyżej.

Dane dotyczące kontroli obecności i geolokalizacji:

Firma Convergent może wprowadzić środki służące do rejestrowania czasu pracy, obecności i punktualności przy użyciu technik opartych na przetwarzaniu danych osobowych dotyczących biometrii, obrazu i/lub geolokalizacji. Takie przetwarzanie danych będzie oparte na wyraźnej zgodzie współpracownika, która zostanie wcześniej uzyskana w umowie o pracę i odpowiednich załącznikach do niej. W każdym przypadku poinformujemy pracownika o rodzaju stosowanego systemu biometrycznego, okresie przechowywania przetwarzanych danych osobowych oraz mechanizmach i procedurach, dzięki którym pracownik może wykonywać swoje prawa.

Wymienione dane mogą być przekazywane lub udostępniane zewnętrznym dostawcom usług w celu obsługi systemów kontroli czasu pracy, obecności i punktualności, przy ścisłym przestrzeganiu przepisów LPDP.



Korzystanie z kamer bezpieczeństwa:

Aby sprostać potrzebom i wymaganiom działalności prowadzonej przez firmę Convergent i/lub zapewnić bezpieczeństwo pracowników i mienia firmy, możemy zainstalować kamery bezpieczeństwa na terenie naszych obiektów. Będzie to realizowane przy ścisłym przestrzeganiu obowiązujących przepisów prawa pracy.

Wszelkie dane osobowe gromadzone za pomocą takich systemów nadzoru muszą być uzasadnione koniecznością przetwarzania w celu wypełnienia obowiązków prawnych dotyczących pracownika, a ich celem musi być zapewnienie bezpieczeństwa pracowników, aktywów firmy Convergent oraz jej działalności.

W ramach wypełniania swoich obowiązków prawnych firma Convergent podejmie odpowiednie środki techniczne i organizacyjne w celu zapewnienia bezpieczeństwa i poufności zebranych danych osobowych. Obrazy lub nagrania mogą zostać zniszczone lub całkowicie usunięte po upływie rozsądnego okresu przechowywania; w żadnym wypadku nie mogą być przechowywane przez czas nieokreślony, chyba że istnieje nakaz sądowy lub równoważny dokument wymagający od nas przechowywania ich przez dłuższy okres, po upływie którego zostaną one należycie usunięte.

Prawa osób, których dane dotyczą, w zakresie przetwarzania ich danych osobowych:

Jeśli Pracownik mieszka w Chile, przysługują mu następujące prawa dotyczące przetwarzania danych osobowych. Należy pamiętać, że wykonywanie tych praw podlega warunkom i wyjątkom określonym przez LPDP:

- **Prawo dostępu:** Pracownik może poprosić o potwierdzenie, czy jego dane osobowe są przetwarzane, a jeśli tak, to może dostać kopię tych danych i informacji o: celach przetwarzania; kategoriach odbiorców, którym dane zostały lub zostaną przekazane; okresie przechowywania; źródle danych; a jeśli przetwarzanie opiera się na uzasadnionym interesie, to jakie są te interesy (art. 5 LPDP).
- **Prawo do sprostowania:** Pracownik może zażądać od nas sprostowania swoich danych osobowych, jeśli są one nieprawidłowe, nieaktualne lub niekompletne (art. 6 LPDP).
- **Prawo do usunięcia danych:** W pewnych okolicznościach Pracownik może zażądać usunięcia swoich danych osobowych, między innymi gdy nie są one już niezbędne do celów, dla których zostały zebrane, gdy wycofał swoją zgodę i nie ma innej podstawy prawnej do przetwarzania lub gdy dane zostały przetworzone niezgodnie z prawem (art. 7 LPDP).
- **Prawo do sprzeciwu:** W niektórych przypadkach Pracownik może sprzeciwić się przetwarzaniu swoich danych osobowych, zwłaszcza gdy przetwarzanie opiera się na uzasadnionym interesie firmy Convergent lub gdy dane zostały uzyskane ze źródeł publicznie dostępnych (art. 8 LPDP).
- **Prawo do sprzeciwu wobec zautomatyzowanego podejmowania decyzji indywidualnych:** Pracownik może sprzeciwić się decyzjom opartym wyłącznie na zautomatyzowanym przetwarzaniu jego danych osobowych – w tym profilowaniu – które wywołują skutki prawne dotyczące Pracownika lub mają na niego istotny wpływ, chyba że ma zastosowanie jeden z wyjątków prawnych (art. 8 bis LPDP).



- **Prawo do ograniczenia przetwarzania:** Pracownik może poprosić o tymczasowe zawieszenie przetwarzania swoich danych osobowych, gdy wniosek o sprostowanie, usunięcie lub sprzeciw jest w trakcie rozpatrywania (art. 8 ter LPDP).
- **Prawo do przenoszenia danych:** W przypadku przetwarzania danych w sposób zautomatyzowany i na podstawie zgody Pracownika, Pracownik może zażądać otrzymania swoich danych osobowych w ustrukturyzowanym, powszechnie używanym formacie elektronicznym nadającym się do odczytu maszynowego oraz zażądać ich przekazania bezpośrednio innemu administratorowi danych, jeżeli jest to technicznie wykonalne (art. 9 LPDP).
- **Prawo do wycofania zgody:** Jeśli przetwarzanie danych opiera się na zgodzie Pracownika, może on ją wycofać w dowolnym momencie. Wycofanie zgody nie ma wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem (art. 12 LPDP).

Jak skorzystać ze swoich praw:

Aby skorzystać z któregośkolwiek z powyższych praw, prosimy o przesłanie pisemnego wniosku na adres dataprotectionofficer@convergent.com. Wniosek musi zawierać: imię i nazwisko, konkretne prawo, z którego Pracownik chce skorzystać oraz informacje umożliwiające identyfikację danych osobowych lub przetwarzania, których dotyczy wniosek. W stosownych przypadkach można dołączyć dokumenty uzupełniające do wniosku. Firma Convergent potwierdzi otrzymanie prośby Pracownika i udzieli pisemnej odpowiedzi w ciągu 30 dni kalendarzowych od daty otrzymania wszystkich niezbędnych dokumentów. Okres ten może zostać przedłużony jednokrotnie o dodatkowe 30 dni kalendarzowych, jeśli wymaga tego złożoność lub liczba wniosków. W takim przypadku Pracownik zostanie o tym poinformowany w odpowiednim terminie.

W przypadku gdy wymaga tego prawo, firma Convergent podejmie uzasadnione środki w celu weryfikacji tożsamości wnioskodawcy przed rozpatrzeniem wniosku.

Prawo do złożenia skargi do organu:

Jeśli Pracownik uważa, że przetwarzanie jego danych osobowych nie jest zgodne z obowiązującymi przepisami, ma prawo złożyć skargę do właściwego organu ochrony danych osobowych w Chile. Po wejściu w życie organem tym będzie Agencja Ochrony Danych Osobowych (APDP). W okresie przejściowym przed 1 grudnia 2026 r. funkcje nadzorcze będą wykonywane zgodnie z obecnymi ramami instytucjonalnymi.

Ponadto, jeśli Pracownik uzna, że akt administracyjny lub ostateczna decyzja wydana przez APDP są niezgodne z prawem, może złożyć skargę bezpośrednio do właściwego sądu apelacyjnego.

KOLUMBIA

Jeśli Pracownik mieszka w Kolumbii, jego dane osobowe są przetwarzane zgodnie z ustawą Ley 1581 de 2012 i jej rozporządzeniami wykonawczymi.

Administratorem danych jest CONVERGINT COLOMBIA SERVICIOS DE INTEGRACIÓN S.A.S. z siedzibą w Bogocie D.C., Kolumbia.



Pracownik ma prawo do:

- dostępu do danych osobowych;
- aktualizowania i poprawiania nieprawidłowych danych;
- żądania usunięcia danych w razie potrzeby;
- cofnięcia upoważnienia, jeśli jest to dozwolone przez prawo;
- składania skarg do Superintendencia de Industria y Comercio.

Wnioski można przesyłać na adres: dataprotectionofficer@convergent.com

MEKSYK

Niniejszy Załącznik dotyczy Pracowników i kandydatów mieszkających w Meksyku. W przypadku jakichkolwiek rozbieżności między niniejszym Załącznikiem a główną Polityką niniejszy Załącznik ma pierwszeństwo.

Firma Convergent przetwarza Dane osobowe zgodnie z federalną ustawą o ochronie danych osobowych będących w posiadaniu osób prywatnych (Ley Federal de Protección de Datos Personales en Posesión de los Particulares), jej przepisami wykonawczymi oraz innymi obowiązującymi meksykańskimi przepisami dotyczącymi ochrony danych („meksykańska ustawa o ochronie danych”).

Administrator danych

Administratorem danych jest odpowiedni podmiot Convergent zatrudniający Pracownika lub otrzymujący aplikację kandydata w Meksyku („Administrator”).

Prawa ARCO

Zgodnie z prawem Meksyku Pracownik ma prawo do:

- Dostępu do Danych osobowych i informacji o ich przetwarzaniu;
- poprawienia nieprawidłowych lub niekompletnych danych;
- usunięcia Danych osobowych, gdy jest to dozwolone przez prawo;
- sprzeciwienia się przetwarzaniu swoich Danych osobowych z prawnie uzasadnionych powodów;
- cofnięcia swojej zgody w zakresie dozwolonym przez prawo.

Aby skorzystać z tych praw, prosimy o kontakt pod adresem: dataprotectionofficer@convergent.com. Wniosek musi zawierać imię i nazwisko, dowód tożsamości (lub pełnomocnictwo), jasny opis danych, których dotyczy wniosek, oraz dane kontaktowe, pod które zostanie wysłana odpowiedź. Wnioski będą rozpatrywane w terminach określonych przez obowiązujące prawo.



Wrażliwe dane osobowe

W razie potrzeby Administrator danych uzyska wyraźną zgodę na przetwarzanie Wrażliwych danych osobowych zgodnie z definicją zawartą w prawie Meksyku.

Przekazywanie

Dane osobowe mogą być przekazywane na terenie kraju lub za granicę zgodnie z główną Polityką. W przypadkach wymaganych przez prawo Meksyku przed dokonaniem takiego przekazania danych zostanie uzyskana zgoda Pracownika, chyba że ma zastosowanie wyjątek prawny.

Skargi

Jeśli Pracownik uważa, że jego prawa do ochrony danych zostały naruszone, może złożyć skargę do Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI).

BRAZYLIA

Niniejszy Załącznik dotyczy Pracowników i kandydatów mieszkających w Brazylii. W przypadku jakichkolwiek rozbieżności między niniejszym Załącznikiem a główną Polityką niniejszy Załącznik ma pierwszeństwo w odniesieniu do przetwarzania Danych osobowych podlegających brazylijskiej ustawie o ochronie danych osobowych (ustawa nr 13 709/2018 lub „LGPD”).

Przetwarzaniem danych osobowych zajmuje się firma **Convergent Comércio e Serviços de Tecnologia Ltda (CNPJ: 58.619.404/0001-48)**.

W przypadku pytań lub potrzeby uzyskania wyjaśnień dotyczących przetwarzania danych osobowych, prosimy o kontakt z Inspektorem Ochrony Danych („DPO”) pod adresem <https://convergent.com.br/lqpd/> lub pocztą elektroniczną pod adresem privacidade-br@convergent.com.

PODSTAWA PRAWNA

Spółka przetwarza Dane osobowe Pracownika w ścisłej zgodności z podstawami prawnymi określonymi w LGPD. W zależności od kontekstu przetwarzania opieramy się na:

- realizacji umowy lub procedur przedumownych: potrzebach w celu rekrutacji, zatrudnienia, zarządzania zatrudnieniem, płacami i świadczeniami pracowniczymi.
- zgodności z obowiązkami prawnymi lub regulacyjnymi: w szczególności w odniesieniu do przepisów prawa pracy, podatków, ubezpieczeń społecznych (w tym, w stosownych przypadkach, systemów sprawozdawczości, takich jak eSocial) oraz bezpieczeństwa i higieny pracy (np. ASO/PCMSO).
- regularnym korzystaniu z praw: w postępowaniach sądowych, administracyjnych lub arbitrażowych.
- uzasadnionych interesach: w celu zapewnienia bezpieczeństwa, monitorowania aktywów przedsiębiorstwa, wewnętrznego zarządzania i zapobiegania nadużyciom, z zastrzeżeniem oceny konieczności i proporcjonalności.



- konieczności ochrony życia lub bezpieczeństwa fizycznego: w stosownych przypadkach
- zgodzie: w przypadkach wymaganych przez prawo w odniesieniu do określonych działań, takich jak niektóre zastosowania marketingowe lub śledzenie geolokalizacji na urządzeniach osobistych. w przypadku, gdy opieramy się na zgodzie, Pracownik ma prawo ją wycofać w dowolnym momencie, z zastrzeżeniem ograniczeń prawnych lub umownych.

WRAŻLIWE DANE OSOBOWE I OSOBY NIELETNIE

- Dane wrażliwe: Przetwarzanie wrażliwych danych osobowych (np. danych dotyczących zdrowia, danych biometrycznych, przynależności do związków zawodowych, pochodzenia rasowego lub etnicznego, wyznania, poglądów politycznych lub orientacji seksualnej) jest ograniczone do minimum niezbędnego do wypełnienia obowiązków prawnych lub regulacyjnych; gdy jest to konieczne w celu zapobiegania oszustwom, prowadzenia dochodzeń dotyczących zgodności z przepisami lub ograniczania ryzyka; gdy jest to wymagane do kontroli dostępu lub środków bezpieczeństwa (w tym stosowania systemów biometrycznych, w stosownych przypadkach); lub na podstawie wyraźnej i podkreślonej zgody, jeżeli jest ona wymagana przez prawo.
- Dane osób nieletnich: W przypadku przetwarzania danych osobowych osób pozostających na utrzymaniu użytkownika, które są nieletnie (np. w celu uzyskania ubezpieczenia zdrowotnego lub świadczeń rodzinnych), dane te muszą być przekazane przez rodzica lub opiekuna prawnego w najlepszym interesie nieletniego.

PRZYNIĘŚ SWOJE WŁASNE URZĄDZENIE (BYOD)

W przypadku, gdy Pracownicy korzystają z urządzeń osobistych do celów zawodowych w ramach programu „Bring Your Own Device” („BYOD”) firmy, Dane osobowe mogą być przetwarzane w celu zapewnienia bezpieczeństwa informacji, ochrony danych poufnych, kontroli dostępu, śledzenia czasu pracy (w stosownych przypadkach) oraz zgodności z wewnętrznymi zasadami. Takie przetwarzanie:

- jest ograniczone do tego, co jest absolutnie konieczne i proporcjonalne do zamierzonego celu biznesowego;
- nie obejmuje nieograniczonego dostępu do treści osobistych niezwiązanych z działalnością zawodową;
- opiera się na odpowiedniej podstawie prawnej zgodnie z LGPD, takiej jak konieczność wynikająca z umowy, obowiązek prawny lub uzasadniony interes, stosownie do przypadku;
- w razie potrzeby może zostać sformalizowane w umowach o pracę lub powiązanych załącznikach do umów;
- podlega zabezpieczeniom technicznym i organizacyjnym mającym na celu ochronę prywatności Pracownika.

W przypadku wdrożenia systemów biometrycznych, geolokalizacji lub narzędzi do zarządzania urządzeniami na urządzeniach osobistych, ich użycie będzie ograniczone do kontekstów



zawodowych i zgodne z brazylijskimi przepisami dotyczącymi ochrony danych i przepisów prawa pracy.

MIĘDZYNARODOWE PRZEKAZYWANIE DANYCH

Dane osobowe mogą być przekazywane poza Brazylię, w tym do innych podmiotów należących do grupy Convergint lub dostawców usług w chmurze. Zgodnie z LGPD międzynarodowe przekazywanie danych może mieć miejsce wyłącznie w przypadkach, gdy:

- kraj docelowy zapewnia odpowiedni poziom ochrony uznany przez ANPD; lub
- wdrożono odpowiednie zabezpieczenia, w tym standardowe klauzule umowne lub inne mechanizmy zatwierdzone przez ANPD; lub
- obowiązuje inna podstawa prawna zgodnie z LGPD.

Korzystanie z infrastruktury w chmurze utrzymywanej poza Brazylią stanowi międzynarodowe przekazywanie danych zgodnie z prawem brazylijskim. W celu ochrony takiego przekazywania wdrażane są odpowiednie zabezpieczenia techniczne, organizacyjne i umowne.

PRAWA

Zgodnie z LGPD Pracownik ma prawo do:

- potwierdzenia istnienia przetwarzania;
- dostępu do danych osobowych;
- korekty niekompletnych, niedokładnych lub nieaktualnych danych;
- anonimizacji, blokowania lub usuwania zbędnych lub nadmiernych danych lub danych przetwarzanych niezgodnie z LGPD.
- przenoszenia danych do innego dostawcy usług na wyraźne żądanie, o ile jest to technicznie wykonalne i zgodne z przepisami ANPD;
- usunięcia danych przetwarzanych na podstawie zgody (z zastrzeżeniem obowiązków prawnych dotyczących przechowywania danych);
- uzyskania informacji o podmiotach publicznych i prywatnych, którym Administrator udostępnił dane osobowe Pracownika.
- uzyskania informacji o możliwości odmowy wyrażenia zgody i konsekwencjach takiej odmowy;
- cofnięcia zgody.
- przeglądu decyzji automatycznych podejmowanych wyłącznie na podstawie



automatycznego przetwarzania danych osobowych, które mają wpływ na interesy Pracownika.

Wnioski można przysyłać na adres privacidade-br@convergint.com. Przed realizacją jakiegokolwiek wniosku możemy wymagać weryfikacji tożsamości, a niektóre wnioski mogą zostać odrzucone, jeśli przechowywanie Danych osobowych jest wymagane przez obowiązujące prawo, w tym przepisy dotyczące pracy, podatków, ubezpieczeń społecznych lub przedawnienia.

Na żądanie można również uzyskać informacje dotyczące konkretnych celów przetwarzania, formy i czasu trwania przetwarzania (z zastrzeżeniem ograniczeń wynikających z tajemnicy handlowej) oraz tożsamości i obowiązków podmiotów przetwarzających dane zgodnie z wymogami LGPD.

Pracownik ma również prawo złożyć skargę do brazylijskiego organu ochrony danych (ANPD).

PRZECHOWYWANIE DANYCH

Dane osobowe są przechowywane zgodnie z obowiązującymi brazylijskimi wymogami prawnymi i regulacyjnymi.

Brazylijskie przepisy dotyczące pracy i podatków nakładają obowiązkowe okresy przechowywania niektórych dokumentów związanych z zatrudnieniem, które mogą trwać nawet do kilku lat po zakończeniu stosunku pracy.

W przypadku, gdy przechowywanie danych jest wymagane w celu wypełnienia obowiązków prawnych lub regularnego wykonywania praw, wnioski o usunięcie danych mogą nie zostać natychmiast zrealizowane.

POWIADOMIENIE O NARUSZENIU BEZPIECZEŃSTWA DANYCH

Zgodnie z LGPD incydenty związane z bezpieczeństwem, które mogą spowodować istotne ryzyko lub szkody dla osób, których dane dotyczą, muszą być zgłaszane do ANPD oraz, w stosownych przypadkach, do osób, których dotyczą.

Firma Convergint stosuje procedury oceny, zarządzania i powiadamiania o incydentach związanych z bezpieczeństwem zgodnie z brazylijskim prawem.

ZAŁĄCZNIK VI: Bliski Wschód

Jeśli Pracownik przebywa poza Królestwem Arabii Saudyjskiej, prosimy o kontakt pod adresem dataprotectionofficer@convergint.com, aby dowiedzieć się więcej o prawach dotyczących prywatności, które mogą mu przysługiwać. Jeśli Pracownik jest mieszkańcem Królestwa Arabii Saudyjskiej, naszym obowiązkiem jest przekazanie mu informacji na temat podstaw prawnych dla przetwarzania jego Danych osobowych i poinformowanie go o przysługujących mu prawach dotyczących prywatności.

Podstawa prawna: Zbierając Dane osobowe bezpośrednio od Pracownika, opieramy się na następujących podstawach prawnych:



- a. za zgodą Pracownika;
- b. w celu spełnienia obowiązku prawnego lub regulacyjnego; i
- c. przestrzeganie umowy zawartej między nami a Pracownikiem.

Zbierając Dane osobowe niebezpośrednio od Pracownika, opieramy się na następujących podstawach prawnych:

- a. Dane osobowe Pracownika są publicznie dostępne lub zebrane z publicznie dostępnego źródła;
- b. zaniechanie zbierania lub przetwarzania Danych osobowych Pracownika może naruszyć jego żywotne interesy; i
- c. Dane osobowe Pracownika są zapisane i przechowywane w formacie, który uniemożliwia jego identyfikację, bezpośrednio lub pośrednio; oraz

niezależnie od tego, czy gromadzimy Dane osobowe od Pracowników, czy od stron trzecich, możemy je również przetwarzać w naszych uzasadnionych interesach. Te uzasadnione interesy zostały opisane w głównej Polityce powyżej.

Opieramy się na uzyskanej od Pracownika zgodzie, jeśli i w takim zakresie, w jakim żadna z powyższych podstaw prawnych opisanych powyżej nie pokrywa konkretnej czynności przetwarzania danych.

Prawa osób, których dane dotyczą: Jeśli Pracownik przebywa poza Królestwem Arabii Saudyjskiej, prosimy o kontakt pod adresem dataprotectionofficer@convergint.com, aby dowiedzieć się więcej o prawach dotyczących prywatności, które mogą mu przysługiwać.

Pracownicy zatrudnieni w KSA mają określone prawa wynikające z ustawy KSA PDPL. Zostały one określone poniżej. Należy jednak pamiętać, że nie są to prawa bezwzględne. Istnieją ich ograniczenia, a niektóre z nich mogą nie być dostępne dla Pracownika w odniesieniu do wszystkich Danych osobowych przetwarzanych przez Spółkę.

Prawo do informacji – Pracownik ma prawo do otrzymania informacji o tym, w jaki sposób wykorzystujemy jego dane oraz o przysługujących mu prawach. Dlatego też przekazujemy Pracownikowi informacje zawarte w niniejszej Polityce.

Prawo do dostępu – Pracownik ma prawo do uzyskania dostępu do swoich Danych osobowych i otrzymania ich kopii (jeśli je przetwarzamy) i niektórych innych informacji (podobnych do tych podanych w niniejszej Polityce).

Prawo do usunięcia – to prawo umożliwia Pracownikowi zażądania usunięcia jego Danych osobowych, jeśli nie ma istotnego powodu, abyśmy nadal z nich korzystali. Nie jest to ogólne prawo do usunięcia danych; istnieją wyjątki.

Prawo do sprostowania – Pracownik ma prawo do sprostowania swoich Danych osobowych, jeśli są one niedokładne lub niekompletne.



Prawo do zgody – jeśli Pracownik wyraził zgodę na przetwarzanie danych, ma prawo do jej wycofania.

Prawo do sprzeciwu – Pracownik ma prawo sprzeciwić się niektórym rodzajom przetwarzania, w tym przetwarzaniu w bezpośrednich celach marketingowych.

Aby złożyć taki wniosek lub sprzeciw, należy wysłać wiadomość e-mail na adres dataprotectionofficer@convergint.com.

Co do zasady odpowiemy na wszystkie wnioski o wykonanie praw osoby, której dane dotyczą, w ciągu 30 dni od otrzymania wszelkich niezbędnych informacji. W okolicznościach, w których nie będziemy w stanie zrealizować wniosku Pracownika lub jeśli realizacja wniosku będzie wymagało dodatkowego czasu, poinformujemy o tym Pracownika na piśmie. W przypadku gdy nie będziemy w stanie w pełni zrealizować wniosku Pracownika (jeśli, na przykład, Dane osobowe Pracownika okażą się powiązane z danymi innej osoby fizycznej, uniemożliwiając ich oddzielenie bez ujawniania Danych osobowych drugiej osoby), udzielimy mu wyjaśnienia w zakresie dozwolonym przez obowiązujące prawo.

Gdy jest to właściwe lub wymagane przez prawo, podejmiemy uzasadnione kroki w celu zweryfikowania tożsamości Pracownika przed udzieleniem odpowiedzi na jego żądania. Etapy weryfikacji mogą się różnić w zależności od wrażliwości Danych osobowych.