ADP Privacy Code dla celów świadczenia Usług Przetwarzania Danych Klienta

ADP Privacy Code dla celów świadczenia Usług Przetwarzania Danych Klienta

Wprowadzenie

ADP świadczy na rzecz Klientów szeroką gamę usług zarządzania kapitałem ludzkim. W opracowanym przez siebie **ADP Code dla Postępowania i Etyki w Biznesie** ADP zobowiązało się do zapewnienia ochrony Danych Osobowych.

Niniejszy ADP Privacy Code (zwany również "Kodeksem") na potrzeby świadczenia Usług Przetwarzania Danych określa, jak to zobowiązanie przekłada się na Przetwarzanie przez ADP Danych Osobowych dotyczących Pracowników Klienta w związku ze świadczeniem Usług dla Klienta oraz Czynności Wsparcia Klienta. W ramach tej struktury Dane Klienta są Przetwarzane przez ADP jako Przetwarzającego Dane w imieniu jego Klientów.

Zasady mające zastosowanie do Przetwarzania przez ADP Danych Osobowych w charakterze Administratora Danych w odniesieniu do Osób Fizycznych, z którymi ADP łączy relacja biznesowa (np. Osób Fizycznych reprezentujących Klientów, Dostawców, Kontrahentów ADP, innych Specjalistów oraz Konsumentów) oraz inne Osoby Fizyczne, których Dane Osobowe są przetwarzane przez ADP w kontekście wykonywanej działalności gospodarczej w charakterze Administratora Danych, określa ***ADP Privacy Code for Business Data.***

Artykuł 1 – Zakres, zastosowanie i wdrożenie

Zakres – Zastosowanie do Danych w EOG	**1.1**	Niniejszy Kodeks dotyczy kwestii Przetwarzania Danych Osobowych Pracowników Klienta przez ADP w charakterze Przetwarzającego Dane na rzecz Klientów w toku świadczenia Usług dla Klienta, jeżeli takie Dane Osobowe (a) podlegają Obowiązującym Przepisom w EOG (lub podlegały Obowiązującym Przepisom w EOG przed przekazaniem takich Danych Osobowych Spółce Grupy poza EOG w kraju, którego właściwe instytucje EOG nie uznawały za zapewniający odpowiedni poziom ochrony danych); oraz (b) są Przetwarzane na podstawie Umowy o Świadczenie Usług, która wyraźnie przewiduje, że niniejszy Kodeks ma zastosowanie do takich Danych Osobowych. W przypadku wątpliwości co do zastosowania niniejszego Kodeksu, odpowiedni Privacy Steward zasięgnie porady Global Data Privacy and Governance Team przed rozpoczęciem Przetwarzania.
Przetwarzanie w formie elektronicznej i papierowej	**1.2**	Niniejszy Kodeks ma zastosowanie do Przetwarzania Danych Klienta przez ADP metodą elektroniczną oraz w systematycznie dostępnych papierowych systemach archiwizacji.
Zastosowanie przepisów prawa miejscowego	**1.3**	Przyjmuje się, że postanowienia niniejszego Kodeksu nie pozbawiają Pracowników Klienta jakichkolwiek praw lub środków prawnych, które przysługiwałyby im zgodnie z Obowiązującymi Przepisami. Jeżeli Obowiązujące Przepisy przewidują szerszy zakres ochrony niż niniejszy Kodeks, zastosowanie mają właściwe postanowienia Obowiązujących Przepisów. Niniejszy Kodeks stosuje się w przypadkach, gdy zapewnia on szerszy zakres ochrony niż Obowiązujące Przepisy lub zapewnia Osobom Fizycznym dodatkowe zabezpieczenia, prawa lub środki prawne.
Polityki i wytyczne	**1.4**	ADP może uzupełniać niniejszy Kodeks przy pomocy polityk, norm, wytycznych i poleceń spójnych z niniejszym Kodeksem.

Rozliczalność **1.5** Niniejszy Kodeks jest wiążący dla ADP. Odpowiedzialni Członkowie Kierownictwa odpowiadają za przestrzeganie niniejszego Kodeksu przez kierowane przez nich jednostki biznesowe. Personel ADP ma obowiązek przestrzegać zapisów niniejszego Kodeksu.

Data Wejścia w Życie **1.6** Niniejszy Kodeks został zatwierdzony przez General Counsel'a po dostarczeniu przez Global Chief Privacy Officera i został przyjęty przez ADP Executive Commity. Niniejszy Kodeks wchodzi w życie z dniem 11 kwietnia 2018 roku (**Data Wejścia w Życie**). Kodeks (zawierający wykaz Spółek Grupy uczestniczących w Przetwarzaniu Danych Klienta) zostanie opublikowany na stronie internetowej www.adp.com. Będzie on również udostępniany Osobom Fizycznym na żądanie.

Niniejszy Kodeks zostanie wdrożony przez Grupę ADP zgodnie z terminami określonymi w art. 16.

Wcześniejsze polityki **1.7** Niniejszy Kodeks stanowi uzupełnienie polityk prywatności ADP i zastępuje wcześniejsze oświadczenia, o ile są one sprzeczne z niniejszym Kodeksem.

Funkcja Podmiotu Upoważnionego ADP **1.8** Spółka Automatic Data Processing, Inc. powołała ADP Nederland B.V. z siedzibą pod adresem Lylantse Baan 1,2908 LG CAPELLE AAN DEN IJSSEL, Holandia, do pełnienia funkcji Podmiotu Upoważnionego ADP, odpowiedzialnego za egzekwowanie niniejszego Kodeksu w Grupie ADP, a ADP Nederland B.V. przyjmuje tę funkcję.

Artykuł 2 – Umowa o Świadczenie Usług

Umowa o Świadczenie Usług; Podprzetwarzający **2.1** ADP będzie Przetwarzać Dane Klienta wyłącznie na podstawie Umowy o Świadczenie Usług, która uwzględnia bezwzględnie obowiązujące wymogi dotyczące zamówień na podstawie Obowiązujących Przepisów dotyczących Przetwarzających Dane oraz w Uzasadnionych Celach określonych w art. 4.

Podmiot Zamawiający ADP korzysta z usług Podprzetwarzających, zarówno Podprzetwarzających ADP, jak i Zewnętrznych Podprzetwarzających, w normalnym toku świadczenia Usług dla Klienta. Umowy o Świadczenie Usług ADP zezwolą na korzystanie z usług takich Podprzetwarzających, jeżeli Podmiot Zamawiający ADP pozostanie odpowiedzialny wobec Klienta za świadczenia Podprzetwarzających zgodnie z warunkami Umowy o Świadczenie Usług. Postanowienia art. 7 w dalszym zakresie regulują korzystanie z usług Podprzetwarzających.

Rozwiązanie Umowy o Świadczenie Usług **2.2** Po zakończeniu świadczenia Usług dla Klienta, ADP wypełni swe zobowiązania względem Klienta wynikające z Umowy o Świadczenie Usług i dotyczące zwrotu Danych Klienta poprzez przekazanie Klientowi Danych Klienta niezbędnych do zapewnienia ciągłości działalności gospodarczej Klienta (jeżeli dane te nie zostały wcześniej przekazane lub udostępnione Klientowi za pośrednictwem odpowiedniej funkcji produktu, np. możliwości pobrania Danych Klienta).

Po wypełnieniu zobowiązań ADP wynikających z Umowy o Świadczenie Usług, ADP bezpiecznie zniszczy pozostałe kopie Danych Klienta oraz (na żądanie Klienta) potwierdzi wobec Klienta, że dane te zostały zniszczone. ADP może utrzymywać kopię Danych Klienta w zakresie wymaganym Obowiązującymi Przepisami, zgodnie z upoważnieniem Klienta, lub w

zakresie niezbędnym na potrzeby rozstrzygania sporów. ADP będzie odtąd przetwarzać Dane Klienta wyłącznie w zakresie wymaganym w wyżej wskazanych celach. Zobowiązania ADP w zakresie poufności na podstawie odpowiedniej Umowy o Świadczenie Usług pozostają w mocy przez cały okres posiadania przez ADP kopii takich Danych Klienta.

Kontrola mechanizmów rozwiązania Umowy

2.3 W ciągu 30 dni od rozwiązania Umowy o Świadczenie Usług (o ile właściwy Organ Ochrony Danych nie zażąda inaczej), ADP, na żądanie Klienta lub właściwego Organu Ochrony Danych, umożliwi skontrolowanie obiektów, w których dokonywane jest Przetwarzanie, zgodnie z art. 11.2 lub 11.3 (w zależności od przypadku), w celu zweryfikowania, czy ADP przestrzega obowiązków związanych z możliwością rozwiązania umowy nałożonych na nią postanowieniami art. 2.2.

Artykuł 3 – Obowiązki w zakresie zapewnienia zgodności

Polecenia Klienta

3.1 ADP będzie Przetwarzać Dane Klienta w imieniu Klienta wyłącznie zgodnie z postanowieniami Umowy o Świadczenie Usług, stosownie do udokumentowanych poleceń otrzymanych od Klienta oraz w zakresie niezbędnym do zapewnienia zgodności z Obowiązującymi Przepisami.

Zgodność z Obowiązującymi Przepisami

3.2 ADP będzie Przetwarzać Dane Klienta zgodnie z Obowiązującymi Przepisami dotyczącymi Przetwarzających Dane.

ADP będzie niezwłocznie i odpowiednio reagować na prośby o pomoc ze strony Klienta, zgodnie z wymogami obowiązującego prawa, w celu umożliwienia Klientowi wypełnienia jego obowiązków wynikających z Obowiązujących Przepisów dotyczących Administratorów Danych, zgodnie z Umową o Świadczenie Usług.

Brak zgodności; Istotny Niekorzystny Wpływ

3.3 Jeżeli Spółka Grupy poweźmie wiedzę o tym, że Obowiązujące Przepisy dotyczące Przetwarzających Dane w kraju spoza EOG lub jakakolwiek zmiana Obowiązujących Przepisów dotyczących Przetwarzających Dane w kraju spoza EOG lub też polecenie Klienta może mieć istotny niekorzystny wpływ na zdolność ADP do wypełnienia jej zobowiązań wynikających z punktów 3.1, 3.2 lub 11.3, taka Spółka Grupy niezwłocznie powiadomi o tym Podmiot Upoważniony ADP i Klienta, w którym to przypadku Klient będzie miał prawo, zgodnie z niniejszym Kodeksem, do tymczasowego wstrzymania przekazywania odpowiednich Danych Klienta do ADP do czasu dostosowania czynności Przetwarzania w celu usunięcia zaistniałego braku zgodności. Jeżeli takie dostosowanie nie będzie możliwe, Klient będzie mógł zrezygnować z odpowiedniej części Przetwarzania przez ADP, zgodnie z warunkami Umowy o Świadczenie Usług. Powyższe prawa i obowiązki nie mają zastosowania, gdy okoliczności lub zmiany Obowiązujących Przepisów dotyczących Przetwarzających Dane wynikają z Wymogów Obowiązkowych.

Żądanie ujawnienia Danych Klienta

3.4 Jeżeli ADP otrzyma żądanie ujawnienia Danych Klienta od organu ścigania lub krajowego organu bezpieczeństwa w kraju spoza EOG (Organ), w pierwszej kolejności oceni dla każdego przypadku z osobna, czy takie żądanie jest prawomocne i wiążące dla ADP. Wszelkie żądania, które nie są w świetle prawa prawomocne i wiążące dla ADP, będą odrzucane zgodnie z Obowiązującymi Przepisami.

Z zastrzeżeniem poniższego ustępu, ADP niezwłocznie powiadomi Klienta,

Wiodący OOD i OOD właściwy dla Klienta zgodnie z art. 11.3 o jakimkolwiek żądaniu ze strony takich Organów, które jest ważne i wiążące dla ADP, i zwróci się do tego Organu z wnioskiem o wstrzymanie tego żądania przez racjonalny okres czasu, tak aby Wiodący OOD mógł wydać opinię dotyczącą zasadności żądania ujawnienia.

Jeżeli zawieszenie wykonania i/lub zawiadomienia do Wiodącego OOD ważnego i wiążącego wniosku o ujawnienie danych jest zabronione, jak w przypadku przewidzianego prawem karnym zakazu w celu zachowania w tajemnicy śledztwa prowadzonego przez organy śledcze, ADP zwróci się do Organu z wnioskiem o zniesienie tego zakazu i udokumentuje fakt złożenia tego wniosku. ADP będzie co roku przekazywać Wiodącemu OOD ogólne informacje o liczbie i rodzajach żądań ujawnienia danych, które otrzymała od Organów w okresie ostatnich 12 miesięcy.

Postanowienia niniejszego artykułu nie mają zastosowania do wniosków otrzymywanych przez ADP od organów w normalnym toku jego działalności jako dostawcy usług zarządzania kapitałem ludzkim (takie jak zajęcie wynagrodzenia), które ADP może w dalszym ciągu świadczyć zgodnie z Obowiązującymi Przepisami, Umową o Świadczenie Usług i dyspozycjami Klientów.

Zapytania ze strony Klientów **3.5** ADP będzie niezwłocznie i odpowiednio reagowało na zapytania Klienta dotyczące Przetwarzania Danych Klienta zgodnie z warunkami Umowy o Świadczenie Usług.

Artykuł 4 – Cele Przetwarzania Danych

Uzasadnione cele biznesowe **4.1** ADP Przetwarza Dane Osobowe (w tym Szczególne Kategorie Danych) dotyczące Pracowników Klienta w zakresie niezbędnym do świadczenia Usług dla Klienta, Czynności Wsparcia Klienta oraz w następujących celach dodatkowych:

(a) hosting, przechowywanie oraz inne formy Przetwarzania niezbędne do zapewnienia ciągłości działania i odzyskania danych po awarii, w tym sporządzenie zapasowych i archiwalnych kopii Danych Osobowych;

(b) administrowanie systemami i siecią oraz ich bezpieczeństwo, w tym monitorowanie infrastruktury, zarządzanie tożsamością i uprawnieniami, weryfikacja i uwierzytelnianie, a także kontrola dostępu;

(c) monitorowanie i inne mechanizmy kontroli niezbędne w celu zapewnienia bezpieczeństwa i integralności transakcji (np. operacji finansowych i przepływu środków pieniężnych), w tym należytej staranności (np. weryfikacji tożsamości Osoby Fizycznej oraz uprawnień tej Osoby Fizycznej do otrzymania produktów lub usług (np. weryfikacji statusu zatrudnienia lub konta);

(d) wykonywanie umów i ochrona ADP, jej Pracowników, Klientów, Pracowników Klienta oraz społeczeństwa przed kradzieżami, odpowiedzialnością prawną, oszustwami i nadużyciami, w tym: (i) wykrywanie, prowadzenie dochodzeń, zapobieganie i minimalizowanie szkód w następstwie oszustw finansowych, kradzieży tożsamości lub usiłowania popełnienia tych czynów oraz innych zagrożeń dla integralności finansowych i fizycznych składników majątku, danych dostępowych oraz

systemów informatycznych; (ii) udział w zewnętrznych inicjatywach dotyczących cyberbezpieczeństwa oraz zapobiegania oszustwom i praniu pieniędzy; oraz (iii) czynności niezbędne do ochrony żywotnych interesów Osób Fizycznych poprzez ostrzeganie Osób Fizycznych przed stwierdzonymi zagrożeniami;

(e) realizacja i zarządzanie wewnętrznymi procesami ADP skutkujące ubocznym Przetwarzaniem Danych Klienta na potrzeby:

(1) kontroli wewnętrznych i sprawozdawczości skonsolidowanej;

(2) zgodności z przepisami prawa, w tym obowiązkowego składania, wykorzystywania i ujawniania informacji wymaganych Obowiązującymi Przepisami;

(3) de-identyfikacji i agregacji zdeidentyfikowanych danych na potrzeby minimalizacji danych i analizy usług;

(4) wykorzystywania zdeidentyfikowanych i zagregowanych danych, za zgodą Klientów, w celu usprawnienia procesów analitycznych, zapewnienia ciągłości i udoskonalania produktów i usług ADP; oraz

(5) usprawniania zarządzania przedsiębiorstwami, w tym fuzji, przejęć, zbyć i wspólnych przedsięwzięć.

Artykuł 5 – Wymagania dotyczące bezpieczeństwa

Bezpieczeństwo danych **5.1** ADP będzie używać racjonalnych i odpowiednich środków technicznych, fizycznych i organizacyjnych w celu zabezpieczenia Danych Klienta przed niewłaściwym wykorzystaniem lub przypadkowym, bezprawnym lub nieuprawnionym zniszczeniem, utratą, modyfikacją, ujawnieniem, pozyskaniem lub dostępem w trakcie Przetwarzania, które to środki będą spełniały wymogi Obowiązujących Przepisów w EOG lub jakiekolwiek bardziej rygorystyczne wymogi, wynikające z Umowy o Świadczenie Usług. ADP w każdym przypadku podejmie kroki określone w Załączniku Nr 2 do niniejszego Kodeksu, które mogą być modyfikowane przez ADP, o ile takie zmiany w sposób istotny nie zawężają zakresu ochrony Danych Klienta przewidzianego w Załączniku Nr 2.

Dostęp do Danych i Poufność **5.2** Personel będzie miał prawo dostępu do Danych Klienta wyłącznie w zakresie niezbędnym do realizacji odpowiednich celów przetwarzania danych przewidzianych w artykule 4. Personel ADP mający dostęp do Danych Klientów zostanie zobowiązany do zachowania poufności.

Powiadomienia o Naruszeniu Bezpieczeństwa Danych **5.3** ADP powiadomi Klienta o Naruszeniu Bezpieczeństwa Danych niezwłocznie po stwierdzeniu wystąpienia takiego naruszenia, chyba że funkcjonariusz organu ścigania lub organ nadzorczy uzna, że takie powiadomienie mogłoby utrudnić dochodzenie lub zagrażałoby bezpieczeństwu narodowemu bądź spowodowałoby naruszenie zaufania do danego sektora gospodarki. W takim przypadku powiadomienie zostanie opóźnione zgodnie z instrukcjami takiego funkcjonariusza organu ścigania lub członka kadry kierowniczej organu nadzorczego. ADP będzie niezwłocznie reagować na zgłoszenia Klientów dotyczące takiego Naruszenia Bezpieczeństwa Danych.

Artykuł 6 – Przejrzystość względem Pracowników Klienta

Inne wnioski Pracowników Klienta

6.1 ADP niezwłocznie powiadomi Klienta o wnioskach lub skargach dotyczących Przetwarzanie Danych Osobowych przez ADP, które wpłynęły bezpośrednio od Pracowników Klienta, jednak nie będzie ustosunkowywać się do tych wniosków lub skarg, o ile nie przewiduje tego Umowa o Świadczenie Usług lub nie zobowiąże jej do tego Klient.

Jeżeli Klient zobowiąże ADP w Umowie o Świadczenie Usług do ustosunkowywania się do wniosków i skarg Pracownika Klienta, ADP zapewni, aby Pracownicy Klienta otrzymali wszystkie informacje racjonalnie niezbędne (takie jak dane osób do kontaktu i sposób postępowania) do skutecznego złożenia takiego wniosku lub skargi przez tego Pracownika Klienta.

Postanowienia niniejszego artykułu 6.1 nie mają zastosowania do wniosków obsługiwanych przez ADP w normalnym toku świadczenia Usług dla Klienta i realizowania Czynności Wsparcia Klienta.

Artykuł 7 – Podprzetwarzający

Umowy z Zewnętrznymi Podprzetwarzającymi

7.1 Zewnętrzni Podprzetwarzający mogą Przetwarzać Dane Klienta wyłącznie na podstawie Umów z Podprzetwarzającymi. Umowa z Podprzetwarzającym nakłada na Zewnętrznego Podprzetwarzającego podobne warunki Przetwarzania dotyczące ochrony danych, które zapewniają nie mniejszy zakres ochrony niż warunki nałożone na Podmiot Zamawiający ADP na podstawie Umowy o Świadczenie Usług i niniejszego Kodeksu .

Publikacja przeglądu kategorii Podprzetwarzających

7.2 ADP opublikuje przegląd kategorii Podprzetwarzających zaangażowanych w świadczenie odpowiednich Usług dla Klienta na odpowiedniej stronie internetowej ADP. Taki przegląd będzie niezwłocznie aktualizowany w przypadku zmian.

Powiadomienia o Nowych Podprzetwarzających i Prawo do Wniesienia Sprzeciwu

7.3 ADP będzie informować Klienta o wszelkich nowych Podprzetwarzających angażowanych przez ADP na potrzeby świadczenia Usług dla Klienta. W ciągu 30 dni od otrzymania takiego zawiadomienia Klient może zgłosić sprzeciw wobec takiego Podprzetwarzającego za pisemnym powiadomieniem ADP, ze wskazaniem obiektywnych, uzasadnionych podstaw niezdolności takiego Podprzetwarzającego do ochrony Danych Klienta zgodnie z odpowiednimi obowiązkami określonymi w Umowie z Podprzetwarzającym, o której mowa w artykule 7.1. Jeżeli Strony nie zdołają wypracować wzajemnie satysfakcjonującego rozwiązania, ADP, według własnego uznania, nie zezwoli na dostęp danego Podprzetwarzającego do Danych Klienta lub umożliwi Klientowi rezygnację z odpowiednich Usług dla Klienta zgodnie z postanowieniami niniejszej Umowy o Świadczenie Usług.

Wyjątek

7.4 Postanowienia niniejszego Punktu 7 nie mają zastosowania w przypadku, gdy Klient zobowiązał ADP do zezwolenia Osobie Trzeciej na Przetwarzanie Danych Klienta na podstawie umowy, którą Klient zawarł bezpośrednio z tą Osobą Trzecią (np. świadczeniodawcą będącym Osobą Trzecią).

Artykuł 8 – Nadzór i zgodność

Global Chief Privacy Officer

8.1 Grupa ADP ustanowi Global Chief Privacy Officera, który będzie odpowiedzialny za:

(a) przewodniczenie posiedzeniom Privacy Leadership Council;

(b) monitorowanie zgodności z niniejszym Kodeksem;

(c) nadzorowanie, koordynowanie, komunikację i konsultacje z odpowiednimi członkami Struktur Poufności w kwestiach poufności i ochrony danych;

(d) składanie Komitetowi Wykonawczemu ADP corocznych raportów z zagrożeń bezpieczeństwa danych i kwestii zgodności;

(e) koordynowanie śledztw i dochodzeń dotyczących Przetwarzania Danych Klienta prowadzonych przez organ administracji rządowej, wspólnie z odpowiednimi członkami Struktur Poufności i Działu Prawnego ADP;

(f) rozstrzyganie sprzeczności pomiędzy niniejszym Kodeksem a Obowiązującymi Przepisami;

(g) monitorowanie procesu Oceny Wpływu na Prywatność (Privacy Impact Assessment; PIA) oraz w razie potrzeby weryfikowanie wyników PIA;

(h) monitorowanie dokumentowania, zgłaszania i komunikowania Naruszeń Bezpieczeństwa Danych;

(i) doradzanie w kwestii procedur, systemów i narzędzi zarządzania danymi na potrzeby wdrożenia mechanizmów zarządzania prywatnością i ochroną danych opracowanych przez Privacy Leadership Council, w tym:

(1) prowadzenie, aktualizowanie i publikowanie niniejszego Kodeksu oraz związanych z nim polityk i standardów;
(2) doradzanie w kwestii narzędzi do gromadzenia, prowadzenia i aktualizowania ewidencji zawierających informacje o strukturze i funkcjonowaniu wszystkich systemów Przetwarzających Dane Klienta;
(3) zapewnianie szkoleń, wsparcia i doradztwa w zakresie szkoleń z dziedziny prywatności danych dla członków Personelu, umożliwiających im zapoznanie się z i wykonywanie ich obowiązków wynikających z niniejszego Kodeksu;
(4) współdziałanie z Działem Kontroli Wewnętrznej ADP oraz innymi jednostkami w celu opracowania i utrzymania odpowiedniego programu kontroli do monitorowania, kontrolowania i zgłaszania zgodności z niniejszym Kodeksem oraz umożliwienia ADP zweryfikowania i potwierdzenia takiej zgodności stosownie do potrzeb;
(5) wdrażanie procedur w zakresie niezbędnym do ustosunkowania się do zapytań, wątpliwości i skarg dotyczących prywatności i ochrony danych; oraz

(6) doradzanie w kwestii odpowiednich kar za naruszenie postanowień niniejszego Kodeksu (np. standardów dyscyplinarnych).

Struktury Poufności

8.2 ADP ustanowi Struktury Poufności odpowiednie do zarządzania przestrzeganiem niniejszego Kodeksu na poziomie globalnym w ADP.

W ramach Struktur Poufności opracowane oraz utrzymywane zostaną

mechanizmy wsparcia dla Global Chief Privacy Officera oraz sprawowany będzie nadzór nad realizacją zadań określonych w artykule 8.1 oraz innych zadań niezbędnych do utrzymywania i aktualizowania niniejszego Kodeksu. Członkowie Struktur Poufności, stosownie do funkcji pełnionej przez siebie w danym regionie lub podmiocie, będą wykonywali następujące zadania dodatkowe:

(a) nadzorowanie wdrażania procedur, systemów i narzędzi zarządzania danymi, które umożliwiają Spółkom Grupy przestrzeganie Kodeksu w poszczególnych regionach i podmiotach;

(b) wspieranie i ocena kompleksowego zarządzania prywatnością i ochroną danych oraz zgodności przez Spółki Grupy w poszczególnych regionach;

(c) regularne doradzanie Privacy Stewardom i Global Chief Privacy Officerowi w zakresie zagrożeń dla poufności danych i kwestii zgodności na szczeblu regionalnym lub lokalnym;

(d) weryfikowanie utrzymywania odpowiednich ewidencji dotyczących systemów Przetwarzających Dane Klienta;

(e) dostępność na potrzeby reagowania na wnioski o zgody dotyczące poufności lub na potrzeby konsultacji;

(f) udzielanie informacji niezbędnych Global Chief Privacy Officerowi do sporządzenia raportu rocznego na temat prywatności;

(g) wspieranie Global Chief Privacy Officera w przypadku wszczęcia przez organy administracji publicznej postępowań wyjaśniających lub skierowania przez nie zapytań;

(h) opracowywanie i publikowanie polityk i standardów dotyczących prywatności właściwych dla poszczególnych regionów lub organizacji;

(i) doradzanie Spółkom Grupy w zakresie przechowywania i niszczenia danych;

(j) zgłaszanie skarg do Global Chief Privacy Officera i pomoc przy ich rozpatrywaniu; oraz

(k) wspieranie Global Chief Privacy Officera, innych członków Struktur Poufności, Privacy Stewardów oraz innych osób, stosownie do potrzeb, w celu:

(1) umożliwienia Spółkom Grupy lub organizacjom przestrzegania Kodeksu przy pomocy opracowanych instrukcji, narzędzi i szkoleń;
(2) rozpowszechniania w regionie najlepszych praktyk z zakresu prywatności i zarządzania ochroną danych;
(3) potwierdzenia, że wymogi dotyczące prywatności i ochrony danych są uwzględniane przy wdrażaniu nowych produktów i usług w Spółkach Grupy i organizacjach; oraz

(4) wspierania Privacy Stewardów, Spółek Grupy, jednostek biznesowych, obszarów funkcjonalnych i personelu ds. zamówień przy pomocy usług Podprzetwarzających.

Privacy Stewardzi

8.3 Privacy Stewardzi to członkowie kadry kierowniczej ADP, którzy zostali powołani przez Odpowiedzialnego Członka Kierownictwa i/lub Wyższe Kierownictwo ADP w celu wdrożenia i egzekwowania niniejszego Kodeksu w

danej jednostce biznesowej lub obszarze funkcjonalnym ADP. Privacy Stewardzi są odpowiedzialni za skuteczne wdrożenie Kodeksu w odpowiednich jednostkach biznesowych lub obszarach funkcjonalnych. W szczególności, Privacy Stewardzi muszą zweryfikować, czy efektywne mechanizmy zarządzania prywatnością i ochroną danych zostały włączone do wszystkich praktyk biznesowych, które mają związek z Danymi Klienta, oraz że dostępne są wystarczające środki i budżet w celu wypełnienia zobowiązań wynikających z niniejszego Kodeksu. Privacy Stewardzi mogą przekazywać zadania i przeznaczać odpowiednie środki na wykonanie nałożonych na nich obowiązków i zrealizowanie założonych celów w zakresie zgodności.

Obowiązki Privacy Stewardów obejmują:

(a) Monitorowanie kompleksowego zarządzania prywatnością i ochroną danych oraz zgodności w przypisanej im Spółce Grupy, jednostce biznesowej lub obszarze funkcjonalnym, oraz weryfikowanie, czy wszystkie procedury, systemy i narzędzia opracowane przez Global Data Privacy and Governing Team zostały skutecznie wdrożone;

(b) Upewnianie się, że zadania dotyczące zarządzania prywatnością i ochroną danych oraz zgodności są należycie przekazywane w toku normalnej działalności, a także w trakcie i po restrukturyzacji organizacji, outsourcingu, fuzjach i przejęciach oraz transakcjach zbycia;

(c) Współpraca z Global Chief Data Officerem oraz odpowiednimi członkami Struktur Poufności w celu zapoznania się i odniesienia się do ewentualnych nowych wymogów prawnych, oraz sprawdzanie, czy procedury zarządzania prywatnością i ochroną danych są aktualizowane, tak aby uwzględniały zmieniające się okoliczności oraz wymogi prawne i regulacyjne;

(d) Współdziałanie z Global Chief Data Officerem i odpowiednimi członkami Struktur Poufności zawsze, kiedy istnieje rzeczywista lub potencjalna sprzeczność pomiędzy Obowiązującymi Przepisami a niniejszym Kodeksem;

(e) Monitorowanie Podprzetwarzających, z których usług korzysta dana Spółka Grupy, jednostka biznesowa lub obszar funkcjonalny w celu potwierdzenia niezmiennego przestrzegania przez tych Podprzetwarzających postanowień niniejszego Kodeksu oraz Umów z Podprzetwarzającymi;

(f) Upewnianie się, że wszyscy członkowie Personelu w danej Spółce Grupy, jednostce biznesowej lub obszarze funkcjonalnym odbyli wymagane szkolenia z zakresu ochrony prywatności; oraz

(g) Nakazywanie usunięcia, zniszczenia, zanonimizowania lub przekazania Danych Klienta zgodnie z postanowieniami artykułu 2.2.

Odpowiedzialni Członkowie Kierownictwa

8.4 Odpowiedzialni Członkowie Kierownictwa, jako szefowie jednostek biznesowych lub obszarów funkcjonalnych, muszą zapewnić wdrożenie w kierowanych przez siebie organizacjach skutecznych mechanizmów zarządzania prywatnością i ochroną danych. Każdy Odpowiedzialny Członek Kierownictwa (a) powoła odpowiednich Privacy Stewardów, (b) zadba o udostępnienie odpowiednich środków i budżetu na potrzeby zgodności, oraz (c) zapewni wsparcie Privacy Stewardom w zakresie niezbędnym do

zaradzenia słabym punktom w obszarze zgodności oraz zarządzania ryzykiem.

Privacy Leadership Council

8.5 Global Chief Privacy Officer przewodniczy Privacy Leadership Council, w której skład wchodzą Privacy Stewardzi, członkowie Struktur Poufności wyznaczeni przez Global Chief Privacy Officera oraz inne osoby, których wsparcie może być niezbędne do realizacji założeń Privacy Leadership Council Privacy Leadership Council opracuje i będzie utrzymywała mechanizmy wsparcia realizacji zadań, w zakresie odpowiednim do zastosowania się przez Spółki Grupy, jednostki biznesowe i obszary funkcjonalne do postanowień niniejszego Kodeksu, do podjęcia zadań w nim przewidzianych oraz w celu wsparcia Global Chief Privacy Officera.

Zastępowanie członków Struktur Poufności i Privacy Stewardów

8.6 Jeżeli w danym czasie nie ma Global Chief Privacy Officera lub nie jest on w stanie wykonywać funkcji właściwych dla tego stanowiska, wówczas General Counsel wyznaczy osobę, która będzie pełniła funkcję tymczasowego Global Chief Privacy Officera. Jeżeli w danym czasie nie ma członka Struktur Poufności dla danego regionu lub organizacji, Global Chief Privacy Officer będzie wykonywał czynności takiego członka Struktur Poufności określone w artykule 8.2.

Jeżeli w danym czasie nie ma Privacy Stewarda dla jakiejkolwiek Spółki Grupy, jednostki biznesowej lub obszaru funkcjonalnego, Odpowiedzialny Członek Kierownictwa wyznaczy odpowiednią osobę do wykonywania czynności określonych w artykule 8.3.

Funkcje przewidziane ustawą

8.7 Jeżeli członkowie Struktur Poufności, np. inspektorzy ochrony danych w świetle Obowiązujących Przepisów w EOG, piastują te stanowiska z mocy prawa, będą oni wykonywali swe obowiązki służbowe, o ile nie koliduje to z wykonywaniem przez nich obowiązków przewidzianych ustawą.

Artykuł 9 – Polityki i procedury

Polityki i procedury

9.1 ADP będzie opracowywać i wdrażać polityki, standardy, wytyczne i procedury w celu zapewnienia zgodności z niniejszym Kodeksem.

Informacje o systemie

9.2 ADP będzie utrzymywać bezpośrednio dostępne informacje na temat struktury i funkcjonowania wszystkich systemów i procesów Przetwarzających Dane Klienta, takie jak ewidencje systemów i procesów mających wpływ na Dane Klienta, wraz z informacjami wygenerowanymi w toku Oceny Skutków dla Ochrony Danych. Kopia takich informacji zostanie przekazana Wiodącemu OOD lub OOD właściwemu dla Klienta zgodnie z artykułem 11.3 na stosowne żądanie.

Artykuł 10 – Szkolenia

Szkolenia

10.1 ADP zapewni szkolenie z zakresu obowiązków i zasad określonych w niniejszym Kodeksie, a także innych obowiązków w zakresie poufności i bezpieczeństwa danych, dla wszystkich członków Personelu mających dostęp do Danych Klienta lub których zakres obowiązków obejmuje Przetwarzanie Danych Klienta.

Artykuł 11 – Zgodność w zakresie monitorowania i audytów

Audyty wewnętrzne

11.1 ADP będzie regularnie weryfikować, czy procesy i procedury biznesowe obejmujące Przetwarzanie Danych Klienta są zgodne z postanowieniami niniejszego Kodeksu. W szczególności:

(a) audyty będą przeprowadzane w toku normalnej działalności Działu Audytu Wewnętrznego ADP (w tym przy pomocy niezależnych Osób Trzecich) oraz innych działów wewnętrznych doraźnie pełniących funkcje kontrolne na żądanie Global Chief Privacy Officera;

(b) Global Chief Privacy Officer może również zażądać, aby audyt został przeprowadzony przez audytora zewnętrznego, a wówczas powiadomi o tym Odpowiedzialnego Członka Kierownictwa danej jednostki biznesowej i/lub Komitet Wykonawczy ADP, w zależności od przypadku;

(c) w trakcie procesu audytowego przestrzegane będą obowiązujące zawodowe standardy niezależności, rzetelności i poufności;

(d) Global Chief Privacy Officer oraz odpowiedni członek Struktur Poufności zostanie powiadomiony o wynikach kontroli;

(e) jeżeli audyt wykaże brak zgodności z niniejszym Kodeksem, wnioski takie zostaną zakomunikowane odpowiednim Privacy Stewardom i Odpowiedzialnym Członkom Kierownictwa. Privacy Stewardzi będą współdziałać z Global Data Privacy and Governance Team w celu opracowania i wykonania odpowiedniego planu naprawczego;

(f) kopia wyników audytu dotycząca zgodności z niniejszym Kodeksem zostanie przekazana Wiodącemu OOD lub właściwemu OOD zgodnie z artykułem 11.3 na stosowne żądanie.

Audyt na żądanie Klienta

11.2 ADP ustosunkuje się do wszelkich wniosków Klienta o przeprowadzenie audytu zgodnie z postanowieniami niniejszego artykułu 11.2. ADP odpowie na zadawane przez Klienta pytania na temat Przetwarzania Danych Klienta przez ADP. Jeżeli Klient racjonalnie oceni, że udzielone przez ADP odpowiedzi uzasadniają dalszą analizę, ADP w porozumieniu z Klientem:

(a) udostępni obiekty wykorzystywane przez siebie do Przetwarzania Danych Klienta na potrzeby audytu przez zewnętrznego, wykwalifikowanego i niezależnego audytora możliwego do przyjęcia dla ADP, zobowiązanego do zachowania poufności w zakresie odpowiadającym ADP i wskazanego do przeprowadzenia audytu przez Klienta. Klient przekaże kopię raportu z audytu Global Chief Privacy Officerowi, a raport ten będzie traktowany jako informacje poufne ADP. Audyty będą przeprowadzane nie częściej niż raz w roku w odniesieniu do danego Klienta w okresie obowiązywania Umowy o Świadczenie Usług, w normalnych godzinach pracy, pod warunkiem (i) wystosowania do ADP pisemnego wniosku co najmniej na 45 dni przed planowaną datą audytu; (ii) zweryfikowania i zatwierdzenia przez pion bezpieczeństwa ADP szczegółowego pisemnego planu audytu; oraz (iii) przestrzegania zasad bezpieczeństwa ADP na terenie zakładu. Audyty takie będą przeprowadzane wyłącznie w obecności przedstawiciela ADP Global Security Office, ADP Global Data Privacy and Governance Team lub innej osoby wyznaczonej przez odpowiedniego przedstawiciela. Audyty takie nie mogą zakłócać czynności ADP w zakresie Przetwarzania ani naruszać bezpieczeństwa i poufności Danych

Osobowych dotyczących innych Klientów ADP; lub

(b) ADP przekaże Klientowi oświadczenie wydane przez zewnętrznego wykwalifikowanego i niezależnego audytora, w którym zaświadcza on, że procesy i procedury biznesowe ADP obejmujące Przetwarzanie Danych Klienta są zgodne z postanowieniami niniejszego Kodeksu.

ADP może zobowiązać Klienta do zapłaty uzasadnionego honorarium za przeprowadzenie takiego audytu.

Niniejszy artykuł 11.2 uzupełnia lub uściśla zakres praw dotyczących audytu przysługujących Klientom na podstawie Obowiązujących Przepisów oraz Umów o Świadczenie Usług. W przypadku jakichkolwiek sprzeczności, moc wiążącą mają postanowienia Obowiązujących Przepisów i Umów o Świadczenie Usług.

Kontrole przeprowadzane przez OOD

11.3 Każdy OOD lub Kraj EOG uprawniony do przeprowadzenia kontroli u Klienta ADP będzie uprawniony do skontrolowania odpowiednich transferów danych pod kątem zgodności z niniejszym Kodeksem, na warunkach, które miałyby zastosowanie do kontroli przeprowadzanej przez ten OOD u Klienta zgodnie z Obowiązującymi Przepisami dotyczącymi Administratorów Danych.

W celu umożliwienia przeprowadzenia takiej kontroli:

(a) ADP i Klient będą współdziałać w dobrej wierze w celu ustosunkowania się do takiego żądania, przekazując OOD informacje, takie jak sprawozdania z audytów ADP, oraz umożliwią komunikację pomiędzy ekspertami z dziedziny danych osobowych z ramienia OOD, Klienta i ADP, którzy zbadają istniejące mechanizmy bezpieczeństwa, prywatności i sterowania operacyjnego. Klient będzie miał dostęp do własnych Danych Klienta zgodnie z postanowieniami Umowy o Świadczenie Usług i może udzielić takiego dostępu przedstawicielom OOD;

(b) jeżeli informacje udostępnione za pomocą takich mechanizmów będą niewystarczające do zrealizowania założeń OOD, ADP umożliwi OOD kontakt z audytorem ADP;

(c) jeżeli okaże się to niewystarczające, ADP udzieli OOD bezpośredniego prawa do przeprowadzenia inspekcji obiektów ADP, w których Przetwarzane są Dane Klienta, z racjonalnym wyprzedzeniem, w normalnych godzinach pracy oraz przy zachowaniu w całkowitej poufności uzyskanych informacji oraz tajemnic handlowych ADP. OOD ma dostęp wyłącznie do Danych Klienta należących do Klienta.

Niniejszy artykuł 11.3 uzupełnia lub uściśla zakres praw dotyczących kontroli przysługujących OOD na podstawie Obowiązujących Przepisów oraz Umów o Świadczenie Usług. W przypadku jakichkolwiek sprzeczności, moc wiążącą mają postanowienia Obowiązujących Przepisów.

Raport roczny

11.4 Global Chief Privacy Officer sporządzi raport roczny dla Komitetu Wykonawczego ADP na temat zgodności z niniejszym Kodeksem, prywatności, zagrożeń dla ochrony danych oraz innych istotnych kwestii. Raport ten będzie zawierał informacje uzyskane od Struktur Poufności oraz innych jednostek na temat procesów lokalnych oraz konkretnych zagadnień w Spółkach Grupy.

Naprawa braku zgodności

11.5 ADP podejmie wszelkie stosowne kroki w celu naprawienia wszelkich przypadków braku zgodności z niniejszym Kodeksem stwierdzonych w trakcie audytu zgodności.

Artykuł 12 – Kwestie prawne

Prawa Pracowników Klienta

12.1 Jeżeli ADP naruszy Kodeks w odniesieniu do Danych Osobowych Pracownika Klienta objętego niniejszym Kodeksem, taki Pracownik Klienta może, jako zewnętrzny beneficjent, wykonać postanowienia artykułów. 1.5, 1.6, 2.1, 2.2, 3, 5, 6, 7.1, 7.3, 7.4, 11.2, 11.3, 12.1, 12.2, 12.3, 12.5, 12.7, 12.8 i 14.3 niniejszego Kodeksu Przetwarzających względem Podmiotu Zamawiającego ADP.

O ile Pracownik Klienta może egzekwować którekolwiek z tych praw względem Podmiotu Zamawiającego ADP, Podmiot Zamawiający ADP, w celu uniknięcia odpowiedzialności, nie może polegać usprawiedliwiaćna naruszeniau jego swoich obowiązków przez ADP przez działaniem w wyniku działania Podprzetwarzającego w celu uniknięcia odpowiedzialności, chyba że obrona praw Podprzetwarzającego może również stanowić obronę praw ADP. ADP może jednak powołać się na jakiekolwiek argumenty obronyprawa, które byłyby dostępne Klientowi. ADP może również powołać się na argumenty obrony, z których ADP mogła skorzystać względem Klienta (takie jak niedbalstwo), przy obronie przed roszczeniem danej poszkodowanej Osoby Fizycznej.

Zgłaszanie i rozpatrywanie skarg

12.2 Pracownicy Klienta mogą złożyć pisemną skargę dotyczącą jakiegokolwiek roszczenia na podstawie artykułu 12.1 do Global Data Privacy and Governance Team drogą pocztową lub mailową na adres wskazany w końcowej części niniejszego Kodeksu. Pracownicy Klienta mogą również składać skargi i roszczenia do odpowiednich organów lub sądów zgodnie z artykułem. 12.3 niniejszego Kodeksu.

Za obsługę skarg i reklamacji odpowiada Global Data Privacy and Governance Team . Każda skarga zostanie przypisana odpowiedniemu członkowi Personelu (w Global Data Privacy and Governance Team lub w odpowiedniej jednostce biznesowej lub obszarze funkcjonalnym). Tacy Członkowie Personelu:

(a) niezwłocznie potwierdzą otrzymanie skargi;

(b) przeanalizują skargę i w razie potrzeby otworzą sprawęrozpoczną postępowanie wyjaśniające;

(c) jeżeli skarga jest uzasadniona, przekażą ją odpowiedniemu Privacy Stewardowi oraz właściwemu członkowi Struktur Poufności w celu opracowania i wdrożenia planu naprawczego; oraz

(d) będą prowadzić ewidencję wszystkich skarg otrzymanych, odpowiedzi udzielonych i czynności naprawczych podjętych przez ADP.

ADP dołoży racjonalnych starań w celu bezzwłocznego rozstrzygnięcia skarg, tak aby Pracownik Klienta otrzymał odpowiedź w ciągu czterech tygodni od dany złożenia skargi. Odpowiedź zostanie sporządzona na piśmie i przesłana do Pracownika Klienta tą samą formą komunikacji, przy pomocy której ten Pracownik Klienta pierwotnie skontaktował się z ADP (np. pocztą lub mailem). Odpowiedź taka będzie określała czynności, jakie ADP podjęła w celu

wyjaśnienia skargi oraz decyzję ADP w kwestii ewentualnych kroków, które podejmie w związku ze skargą.

Jeżeli ADP nie może realnie zakończyć postępowania wyjaśniającego i przedstawić odpowiedzi w ciągu czterech tygodni, ADP powiadomi Pracownika Klienta w ciągu czterech tygodni, że postępowanie jest w toku i że odpowiedź zostanie wystosowana w ciągu kolejnych ośmiu tygodni.

Jeżeli Pracownik Klienta uzna odpowiedź ADP na przedmiotową skargę za niewystarczającą (nptj. wniosek zostanie odrzucony) lub ADP nie zastosuje się do warunków procedury rozpatrywania skarg określonych w artykule. 12.2, Pracownik Klienta może złożyć skargę lub roszczenie do odpowiednich organów lub sądów zgodnie z artykułem. 12.3.

Rozstrzyganie roszczeń Pracowników Klienta

12.3 Pracownicy Klienta powinni w pierwszej kolejności przestrzegać procedury rozpatrywania skarg określonej w artykule. 12.2 niniejszego Kodeksu, przed złożeniem jakiejkolwiek skargi lub podniesienia roszczenia przed odpowiednimi organami lub sądami.

Pracownicy Klienta mogą, wedle uznania, zgłaszać roszczenia zgodnie z artykułem. 12.1, składając skargę do:

(i) OOD w kraju swego zwykłego pobytu, miejsca pracy lub miejsca, w którym doszło do naruszenia, przeciwko Podmiotowi Zamawiającemu ADP lub Podmiotowi Upoważnionemu ADP; lub

(ii) Wiodącego OOD lub sądów holenderskich, przy czym w tym przypadku skarga może zostać złożona wyłącznie przeciwko Podmiotowi Upoważnionemu ADP.

Pracownicy Klienta mogą, wedle uznania, zgłaszać roszczenia zgodnie z artykułem. 12.1, składając skargę do:

(i) sądu w kraju swego zwykłego pobytu lub w kraju, w którym rozpoczął się przedmiotowy transfer danych zgodnie z niniejszym Kodeksem, przeciwko Podmiotowi Zamawiającemu ADP lub Podmiotowi Upoważnionemu ADP; lub

(ii) Wiodącego OOD lub sądów holenderskich, przy czym w tym przypadku skarga może zostać złożona wyłącznie przeciwko Podmiotowi Upoważnionemu ADP.

Do powyższych sporów OOD i sądy będą stosowały własne przepisy prawa materialnego i procesowego. Wybór dokonany przez Pracownika Klienta nie ogranicza ewentualnych praw materialnych i proceduralnych przysługujących stronom na podstawie Obowiązujących Przepisów.

Prawa Klientów

12.4 Klient może egzekwować postanowienia niniejszego Kodeksu wobec (i) Podmiotu Zamawiającego ADP, lub (ii) Podmiotu Upoważnionego ADP przed Wiodącym OOD lub sądami holenderskimi, jednak pod warunkiem, że Podmiot Zamawiający ADP nie został utworzony w Kraju EOG. Podmiot Upoważniony ADP zadba, aby podjęte zostały odpowiednie kroki w celu naprawienia naruszeń niniejszego Kodeksu przez Podmiot Zamawiający ADP lub jakąkolwiek inną Spółkę Grupy.

Podmiot Zamawiający ADP i Podmiot Upoważniony ADP w celu uniknięcia odpowiedzialności, nie mogą usprawiedliwiać naruszenia swoich obowiązków działaniem polegać na naruszeniu obowiązków przez inną Spółkę Grupy lub Podprzetwarzającego w celu uniknięcia odpowiedzialności, chyba że obrona

praw takiej Spółki Grupy lub Podprzetwarzającego może również stanowić obronę praw ADP.

Dostępne środki prawne; ciężar dowodu po stronie Pracowników Klienta

12.5 Jeżeli Pracownikowi Klienta przysługuje roszczenie na podstawie artykułu. 12.1, Pracownikowi Klienta przysługuje odszkodowanie za szkody w zakresie przewidzianym przepisami obowiązującymi w EOG.

Jeżeli Pracownicy Klienta wnoszą roszczenie o odszkodowanie na podstawie artykułu. 12.1, to Pracownicy Klienta mają obowiązek wykazać, że ponieśli szkody oraz ustalić okoliczności wskazujące na duże prawdopodobieństwo, że szkody powstały wskutek naruszenia niniejszego Kodeksu. Następnie Podmiot Zamawiający ADP (lub Podmiot Upoważniony ADP, w zależności od przypadku) ma obowiązek wykazać, że szkody poniesione przez Pracowników Klienta wskutek naruszenia niniejszego Kodeksu nie powstały z winy odpowiedniej Spółki Grupy lub Podprzetwarzającego, lub użyć innych argumentów obrony.

Odszkodowanie dla Klientów

12.6 W przypadku naruszenia postanowień niniejszego Kodeksu, oraz z zastrzeżeniem warunków Umowy o Świadczenie Usług, Klientom będzie przysługiwało prawo do odszkodowania za szkody bezpośrednie, zgodnie z postanowieniami Umowy o Świadczenie Usług.

Wzajemne wsparcie

12.7 Wszystkie Spółki Grupy, w niezbędnym zakresie, będą współpracowały i udzielą wsparcia, na ile to możliwe, przy (a) obsłudze wniosku, skargi lub roszczenia wniesionego przez Klienta lub Pracownika Klienta, lub (b) zastosowania się do wymogów zgodnego z prawem śledztwa lub dochodzenia prowadzonego przez właściwy organ administracji publicznej.

Spółka Grupy otrzymująca wniosek o udzielenie informacji zgodnie z artykułem. 6.1, lub skargę bądź roszczenie zgodnie z artykułem. 12.2 lub 12.3, odpowiada za komunikację z Klientem lub z Pracownikiem Klienta w sprawie takiego wniosku lub roszczenia, o ile okoliczności nie wymagają inaczej lub o ile Global Data Privacy and Governance Team nie wydał odmiennych wytycznych.

Zalecenia i wiążące decyzje OOD

12.8 ADP będzie współdziałać w dobrej wierze i dołoży wszelkich zasadnych starań w celu zastosowania się do zaleceń Wiodącego OOD oraz właściwego OOD zgodnie z art. 12.3 wydanych w sprawie interpretacji i stosowania niniejszego Kodeksu. ADP zastosuje się do wiążących decyzji właściwych OOD.

Prawo właściwe dla niniejszego Kodeksu

12.9 Niniejszy Kodeks podlega przepisom prawa holenderskiego i należy go interpretować zgodnie z tymi przepisami.

Artykuł 13 – Konsekwencje nieprzestrzegania Kodeksu

Brak zgodności

13.1 Nieprzestrzeganie postanowień niniejszego Kodeksu przez członków Personelu może skutkować podjęciem kroków dyscyplinarnych lub sankcji umownych zgodnie z obowiązującymi przepisami i politykami ADP, włącznie z rozwiązaniem stosunku pracy lub stosunku umownego.

Artykuł 14 – Sprzeczność pomiędzy niniejszym Kodeksem a Obowiązującymi Przepisami dotyczącymi Przetwarzających Dane

Sprzeczność pomiędzy niniejszym Kodeksem a obowiązującym Prawem

14.1 W przypadku sprzeczności pomiędzy Obowiązującymi Przepisami dotyczącymi Przetwarzających Dane a niniejszym Kodeksem, Odpowiedzialny Członek Kierownictwa lub Privacy Steward skonsultuje się z Global Chief Privacy Officerem, odpowiednimi członkami Struktur Poufności (w zależności od przypadku) oraz działem prawnym danej jednostki biznesowej w celu ustalenia, jak zapewnić zgodność z niniejszym Kodeksem oraz rozstrzygnięcia sprzeczności w racjonalnie możliwym zakresie, biorąc pod uwagę wymogi prawne mające zastosowanie do ADP.

Nowe sprzeczne wymogi prawne

14.2 Członkowie działu prawnego, ADP Business Security Officerowie oraz Privacy Stewardzi będą niezwłocznie informować Global Data Privacy and Governance Team o wszelkich nowych wymogach prawnych, które, zgodnie z ich wiedzą, mogą wpłynąć na możliwość przestrzegania zapisów niniejszego Kodeksu przez ADP.

Odpowiedni Privacy Stewardzi, w porozumieniu z działem prawnym, będą niezwłocznie informować Odpowiedzialnych Członków Kierownictwa o wszelkich nowych wymogach prawnych, które mogą utrudnić ADP przestrzeganie zapisów niniejszego Kodeksu.

Przekazywanie informacji do Wiodącego OOD

14.3 Jeżeli ADP poweźmie wiedzę o tym, że Obowiązujące Przepisy dotyczące Przetwarzających Dane lub jakakolwiek zmiana Obowiązujących Przepisów dotyczących Przetwarzających Dane może mieć istotny niekorzystny wpływ na zdolność ADP do wypełnienia jej zobowiązań wynikających z artykułów 3.1, 3.2 lub 11.3, ADP powiadomi o tym Wiodący OOD.

Artykuł 15 – Zmiany niniejszego Kodeksu

Zatwierdzanie zmian

15.1 Wszelkie istotne zmiany niniejszego Kodeksu wymagają uprzedniej zgody Global Chief Privacy Officera i General Counsela, oraz zatwierdzenia przez Komitet Wykonawczy ADP, po czym zostaną zakomunikowane Spółkom Grupy. Mniej istotnych zmian Kodeksu można dokonywać za uprzednią zgodą Global Chief Privacy Officera. Podmiot Upoważniony ADP będzie co roku zawiadamiał Wiodący OOD o wszelkich zmianach niniejszego Kodeksu.

Jeżeli jakakolwiek zmiana niniejszego Kodeksu ma istotny wpływ na warunki Przetwarzania dotyczące Usług dla Klienta, ADP niezwłocznie powiadomi o tym Wiodący OOD pokrótce objaśniając taką zmianę oraz poinformuje o niej Klienta. W ciągu 30 dni od otrzymania takiego zawiadomienia Klient może zgłosić sprzeciw wobec takiej zmiany za pisemnym powiadomieniem ADP. Jeżeli strony nie wypracują rozwiązania satysfakcjonującego obie Strony, ADP wprowadzi alternatywną formę przekazywania danych. Jeżeli nie można wprowadzić alternatywnej formy przekazywania danych, Klient będzie mógł, zgodnie z niniejszym Kodeksem, zawiesić dane przekazywanie Danych Klienta do ADP. Jeżeli zawieszenie przekazywania danych nie będzie możliwe, ADP umożliwi Klientowi rezygnację z odpowiedniej części Usług dla Klienta zgodnie z warunkami Umowy o Świadczenie Usług.

Data wejścia w życie zmian

15.2 Wszelkie zmiany wchodzą w życie ze skutkiem natychmiastowym po ich zatwierdzeniu zgodnie z artykułem 15.1, opublikowaniu na stronie www.adp.com i zakomunikowaniu Klientom.

Wcześniejsze wersje **15.3** Wszelkie wnioski, skargi i roszczenia ze strony Pracownika Klienta dotyczące niniejszego Kodeksu będą rozpatrywane dla wersji Kodeksu obowiązującej w chwili złożenia takiego wniosku, skargi lub roszczenia.

Artykuł 16 – Okresy wdrażania i okresy przejściowe

Wdrożenie **16.1** Nad wdrożeniem niniejszego Kodeksu będą czuwać Privacy Stewardzi wspólnie z Global Data Privacy and Governance Team. O ile w dalszej części nie wskazano inaczej, okres przejściowy na zapewnienie zgodności z niniejszym Kodeksem będzie obowiązywał przez okres osiemnastu miesięcy od Daty Wejścia w Życie (zgodnie z zapisami artykułu 1.6).

O ile nie wskazano inaczej, w ciągu osiemnastu miesięcy od Daty Wejścia w Życie, wszelkie czynności Przetwarzania Danych Klienta będą realizowane zgodnie z niniejszym Kodeksem, a Kodeks będzie w pełni ważny i skuteczny. W okresie przejściowym Kodeks zaczyna obowiązywać daną Spółkę Grupy niezwłocznie po zrealizowaniu przez tę Spółkę Grupy zadań niezbędnych do pełnego wdrożenia oraz po uprzednim powiadomieniu Global Chief Privacy Officera Danych przez tę Spółkę Grupy.

Nowe Spółki Grupy **16.2** Każdy podmiot, który stanie się Spółką Grupy po Dacie Wejścia w Życie, ma obowiązek zastosowania się do niniejszego Kodeksu w ciągu dwóch lat od uzyskania statusu Spółki Grupy.

Zbyte Podmioty **16.3** Zbyty Podmiot w dalszym ciągu podlega postanowieniom niniejszego Kodeksu po jego zbyciu przez okres niezbędny ADP do rozdzielenia Przetwarzania Danych Klienta w odniesieniu do takiego Zbytego Podmiotu.

Okres przejściowy dla dotychczasowych umów **16.4** Jeżeli niniejszy Kodeks ma wpływ na jakiekolwiek dotychczasowe umowy z Podprzetwarzającymi lub innymi Osobami Trzecimi, postanowienia tych umów mają znaczenie nadrzędne do czasu ich przedłużenia w normalnym toku działalności, przy czym wszystkie takie dotychczasowe umowy muszą zostać dostosowane do postanowień niniejszego Kodeksu w ciągu 18 miesięcy od Daty Wejścia w Życie.

Dane kontaktowe

ADP Global Data Privacy and Governance Team:
privacy@adp.com

Podmiot Upoważniony ADP
ADP Nederland B.V.
Lylantse Baan 1,2908
LG CAPELLE AAN DEN IJSSEL
HOLANDIA

Interpretacja

INTERPRETACJA NINIEJSZEGO KODEKSU:

(i) O ile kontekst nie wskazuje inaczej, wszelkie odniesienia do określonego artykułu lub Załącznika dotyczą artykułu lub Załącznika w lub do niniejszego dokumentu, z późniejszymi zmianami.

(ii) Nagłówki pełnią jedynie funkcję informacyjną i nie należy ich uwzględniać przy interpretacji jakichkolwiek postanowień niniejszego Kodeksu;

(iii) W przypadku zdefiniowanych terminów lub zwrotów pozostałe ich formy

gramatyczne interpretuje się odpowiednio;

(iv) Wyrazy w rodzaju męskim obejmują również rodzaj żeński;

(v) Określenia „uwzględniają/uwzględnia” oraz „w tym”, a także wszelkie wyrazy po nich następujące interpretuje się bez uszczerbku dla ogólnego charakteru którychkolwiek poprzedzających ich wyrazów lub koncepcji, i vice versa;

(vi) Określenie „pisemne/na piśmie” obejmuje wszelkie udokumentowane formy korespondencji, pisma, kontrakty, zapisy elektroniczne, podpisy elektroniczne, kopie lub inne prawnie wiążące i wykonalne dokumenty bez względu na ich format;

(vii) Odniesienia do dokumentów (w tym, między innymi, odniesienia do niniejszego Kodeksu) dotyczą tych dokumentów z uwzględnieniem ich zmian, modyfikacji, uzupełnień i wymian, za wyjątkiem przypadków, gdy zabrania tego niniejszy Kodeks lub przedmiotowy dokument;

(viii) Odniesienia do przepisów prawa obejmują wszelkie wymogi regulacyjne, zalecenia branżowe oraz najlepsze praktyki publikowane przez właściwe krajowe i międzynarodowe organy nadzoru lub inne podmioty.

ZAŁĄCZNIK NR 1 – Definicje WRK

Decyzja Stwierdzająca Odpowiedni Poziom Ochrony	DECYZJA STWIERDZAJĄCA ODPOWIEDNI POZIOM OCHRONY oznacza jakiekolwiek rozstrzygnięcie Organu Ochrony Danych lub innego właściwego organu stwierdzające, że dany kraj, region lub odbiorca transferu danych zapewnia odpowiedni poziom ochrony Danych Osobowych. Do podmiotów, których dotyczy Decyzja Stwierdzająca Odpowiedni Poziom Ochrony, zalicza się odbiorców znajdujących się w krajach, które zgodnie z Obowiązującymi Przepisami uważane są za kraje zapewniające odpowiedni poziom ochrony danych, a także odbiorców związanych innymi dokumentem (np. Wiążącymi Regułami Korporacyjnymi), który został zatwierdzony przez odpowiedni Organ Ochrony Danych lub inny właściwy podmiot. W przypadku Stanów Zjednoczonych, spółki, które uzyskują certyfikację na potrzeby jakichkolwiek porozumień dotyczących prywatności pomiędzy USA a EOG i/lub USA a Szwajcarią podlegają postanowieniom Decyzji Stwierdzającej Odpowiedni Poziom Ochrony.
ADP (Grupa ADP)	ADP (GRUPA ADP) oznacza łącznie Automatic Data Processing, Inc. (Spółka Dominująca) oraz Spółki Grupy, w tym także ADP, Inc.
Podmiot Zamawiający ADP	PODMIOT ZAMAWIAJĄCY ADP oznacza Spółkę Grupy, która przystąpiła do kontraktu wymaganego Kodeksami, takiego jak Umowa o Świadczenie Usług, Umowa z Podprzetwarzającym lub umowa o przekazywanie danych.
Podmiot Upoważniony ADP	PODMIOT UPOWAŻNIONY ADP oznacza ADP Nederland B.V. z siedzibą pod adresem Lylantse Baan 1, 2908 LG CAPELLE AAN DEN IJSSEL, Holandia.
Komitet Wykonawczy ADP	KOMITET WYKONAWCZY ADP oznacza komitet, w którego skład wchodzą członkowie kadry kierowniczej, tj. (i) Dyrektor Generalny Automatic Data Processing, Inc., oraz (ii) inni członkowie kadry kierowniczej podlegający bezpośrednio Dyrektorowi Generalnemu, którzy łącznie odpowiadają za działalność operacyjną grupy ADP.
Podprzetwarzający ADP	Na potrzeby Privacy Code dla celów świadczenia Usług Przetwarzania Danych Klienta, PODPRZETWARZAJĄCY ADP oznacza jakąkolwiek Spółkę Grupy zaangażowaną przez inną Spółkę Grupy jako Podprzetwarzający w odniesieniu do Danych Klienta.
Obowiązujące Przepisy dotyczące Administratora Danych	Na potrzeby Privacy Code dla celów świadczenia Usług Przetwarzania Danych Klienta, OBOWIĄZUJĄCE PRZEPISY DOTYCZĄCE ADMINISTRATORA DANYCH oznaczają jakiekolwiek przepisy dotyczące ochrony prywatności lub danych mające zastosowanie do Klienta ADP jako Administratora takich Danych Klienta.
Obowiązujące Przepisy dotyczące Przetwarzających Dane	Na potrzeby Privacy Code dla celów świadczenia Usług Przetwarzania Danych Klienta, OBOWIĄZUJĄCE PRZEPISY DOTYCZĄCE PRZETWARZAJĄCYCH DANYCH oznaczają jakiekolwiek przepisy dotyczące ochrony prywatności lub danych mające zastosowanie do ADP jako Przetwarzającego Dane w imieniu Klienta, który jest Administratorem Danych.
Obowiązujące Przepisy	OBOWIĄZUJĄCE PRZEPISY oznaczają wszelkie przepisy dotyczące prywatności lub ochrony danych, które mają zastosowanie do konkretnych czynności Przetwarzania.

Kandydat	KANDYDAT oznacza każdą Osobę Fizyczną udostępniającą ADP Dane Osobowe w kontekście ubiegania się o stanowisko Pracownika ADP.
Archiwum	ARCHIWUM oznacza zbiór Danych Osobowych, które nie są już potrzebne do osiągnięcia celów, dla których te Dane zostały pierwotnie zgromadzone, lub które nie są już wykorzystywane w ogólnej działalności gospodarczej, ale mogą być wykorzystywane do celów historycznych, naukowych lub statystycznych, do rozstrzygania sporów, prowadzenia postępowań wyjaśniających lub do ogólnych celów archiwizacji. Dostęp do Archiwum jest ograniczony do administratorów systemu i innych osób, których obowiązki służbowe wymagają dostępu do archiwum.
Pracownik	PRACOWNIK oznacza Kandydata, aktualnego pracownika ADP lub byłego pracownika ADP, z wyjątkiem Osób Współzatrudnionych. UWAGA: ADP Workplace Privacy Code nie ma zatem zastosowania do Przetwarzania Danych Osobowych Osób Współzatrudnionych.
Automatic Data Processing, Inc.	AUTOMATIC DATA PROCESSING, INC. to jednostka dominująca Grupy ADP, spółka prawa stanu Delaware (USA) z główną siedzibą pod adresem: One ADP Boulevard, Roseland, New Jersey, 07068-1728, USA.
Wiążące Reguły Korporacyjne	WIĄŻĄCE REGUŁY KORPORACYJNE oznaczają politykę prywatności grupy powiązanych spółek, co do której uważa się, że zapewnia odpowiedni poziom ochrony przekazywania Danych Osobowych w ramach tej grupy spółek zgodnie z Obowiązującymi Przepisami.
Służbowe Dane Kontaktowe	SŁUŻBOWE DANE KONTAKTOWE oznaczają jakiekolwiek dane dotyczące danego Specjalisty zwykle zamieszczane na wizytówce lub w stopce maila.
Kontrahent	KONTRAHENT oznacza jakąkolwiek Osobę Trzecią, z wyjątkiem Klienta lub Dostawcy, którą łączy lub łączyła z ADP relacja biznesowa lub sojusz strategiczny (np. partnerstwo marketingowe, wspólne przedsięwzięcie lub partnerstwo przy budowie).
Cel Biznesowy	CEL BIZNESOWY oznacza uzasadniony cel Przetwarzania Danych Osobowych określony w artykule 2, 3 lub 4 któregokolwiek Kodeksu ADP, lub Przetwarzania Szczególnych Kategorii Danych określonych w artykule 4 któregokolwiek Kodeksu ADP.
Dzieci	Na potrzeby gromadzenia danych i marketingu, termin DZIECI oznacza Osoby Fizyczne, które nie ukończyły wieku uznanego w obowiązujących przepisach za wiek umożliwiający udzielenie ważnej zgody na takie gromadzenie danych i/lub czynności marketingowe.
Klient	KLIENT oznacza jakąkolwiek Osobę Trzecią korzystającą z jednego lub większej liczby produktów lub usług ADP w toku prowadzenia własnej działalności.
Dane Klienta	DANE KLIENTA oznaczają Dane Osobowe dotyczące Pracowników Klienta (w tym przyszłych pracowników, byłych pracowników oraz osób pozostających na utrzymaniu pracowników) przetwarzane przez ADP w związku ze świadczeniem Usług dla Klienta.
Pracownik Klienta	PRACOWNIK KLIENTA oznacza jakąkolwiek Osobę Fizyczną, której Dane Osobowe są Przetwarzane przez ADP jako Przetwarzającego Dane na rzecz

	Klienta na podstawie Umowy o Świadczenie Usług. W celu uniknięcia wątpliwości należy podkreślić, że termin PRACOWNIK KLIENTA dotyczy wszystkich Osób Fizycznych, których Dane Osobowe są Przetwarzane przez ADP w ramach świadczenia Usług dla Klienta (niezależnie od charakteru prawnego relacji łączącej daną Osobę Fizyczną z Klientem). Nie dotyczy to Specjalistów, których Dane Osobowe są Przetwarzane przez ADP z racji bezpośredniej relacji łączącej ADP z Klientem. Przykładowo, ADP może Przetwarzać Dane Osobowe Specjalisty ds. Kadr w celu zawarcia umowy z Klientem – takie dane są objęte Privacy Code for Business Data. Jeżeli jednak ADP świadczy na rzecz Klienta usługi Przetwarzania listy płac (np. wydaje odcinki wynagrodzenia, pomaga w obsłudze systemu ADP), dane Osoby Fizycznej będą Przetwarzane jako Dane Klienta.
Usługi dla Klienta	USŁUGI DLA KLIENTA oznaczają usługi zarządzania kapitałem ludzkim świadczone przez ADP na rzecz Klientów, takie jak obsługa procesu rekrutacji, listy płac i wynagrodzeń, świadczeń pracowniczych, zarządzanie talentami, administracja kadr, usługi konsultingowe i analityczne oraz obsługa emerytur.
Czynności Wsparcia Klienta	CZYNNOŚCI WSPARCIA KLIENTA oznaczają czynności Przetwarzania podejmowane przez ADP w celu wsparcia dostawy jej produktów i usług. Czynności Wsparcia Klienta mogą obejmować, między innymi, szkolenie Specjalistów, odpowiadanie na pytania dotyczące usług, otwieranie i zamykanie zgłoszeń serwisowych, udzielanie informacji na temat produktów i usług (w tym aktualizacji i komunikatów o braku zgodności), kontrolę i monitorowanie jakości oraz inne pokrewne czynności umożliwiające efektywne korzystanie z produktów i usług ADP.
Kodeks	KODEKS oznacza (w zależności od przypadku) ADP Privacy Code dla celów Danych Biznesowych, ADP Workplace Privacy Code (dokument wewnętrzny ADP) oraz ADP Privacy Code dla celów świadczenia Usług Przetwarzania Danych Klienta; łącznie zwane Kodeksami.
Osoba Współzatrudniona	OSOBA WSPÓŁZATRUDNIONA oznacza pracownika Klienta z nUSA, który jest współzatrudniony przez amerykański podmiot pośrednio powiązany ze spółką Automatic Data Processing, Inc. w ramach oferty profesjonalnej organizacji pracodawców w Stanach Zjednoczonych.
Konsument	KONSUMENT oznacza Osobę Fizyczną bezpośrednio kontaktującą się z ADP we własnym imieniu. Przykładowo, do grona Konsumentów zaliczają się osoby fizyczne, które uczestniczą w programach rozwoju talentów lub korzystają z produktów i usług ADP w celach prywatnych (tj. poza stosunkiem pracy z ADP lub Klientem ADP).
Pracownik Tymczasowy	PRACOWNIK TYMCZASOWY oznacza Osoby Fizyczne świadczące usługi na rzecz ADP (podlegające bezpośredniemu nadzorowi ADP) na zasadzie przejściowej lub czasowej, takie jak pracownicy tymczasowi, pracownicy kontraktowi, niezależni wykonawcy lub konsultanci.
Administrator Danych	ADMINISTRATOR DANYCH oznacza osobę prawną lub fizyczną, która – samodzielnie lub wspólnie z innymi – określa cele i sposoby Przetwarzania Danych Osobowych.
Przetwarzający Dane	PRZETWARZAJĄCY DANE oznacza osobę prawną lub fizyczną, która

	Przetwarza Dane Osobowe na rzecz Administratora Danych.
Organ Ochrony Danych (OOD)	ORGAN OCHRONY DANYCH (OOD) oznacza jakikolwiek organ regulacyjny lub organ nadzoru sprawujący nadzór nad ochroną lub prywatnością danych w kraju, w którym działa którakolwiek Spółka Grupy.
Ocena Skutków dla Ochrony Danych (DPIA)	OCENA SKUTKÓW DLA OCHRONY DANYCH (DPIA) oznacza procedurę dokonywania i dokumentowania uprzedniej oceny skutków, jakie dane czynności Przetwarzania mogą spowodować w kontekście stopnia ochrony Danych Osobowych, gdy takie czynności Przetwarzania danych osobowych mogą wiązać się z wysokim ryzykiem naruszenia praw i wolności Osób Fizycznych, w szczególności, gdy wykorzystywane są nowe technologie. DPIA zawierać będzie: (i) opis: (a) zakresu i kontekstu Przetwarzania; (b) Celów Biznesowych, dla których Dane Osobowe są Przetwarzane; (c) szczegółowych celów przetwarzania Szczególnych Kategorii Danych; (d) kategorii odbiorców Danych Osobowych, w tym odbiorców, których nie dotyczy Decyzja Stwierdzająca Odpowiedni Poziom Ochrony; (e) okresów przechowywania Danych Osobowych; (ii) ocenę: (a) niezbędności i proporcjonalności Przetwarzania; (b) ryzyka naruszeń praw Osób Fizycznych do ochrony prywatności; oraz środków ograniczania takich ryzyk, w tym zabezpieczeń oraz innych środków i mechanizmów bezpieczeństwa (np. domyślna ochrona prywatności) mających zapewnić ochronę Danych Osobowych.
Naruszenie Bezpieczeństwa Danych	NARUSZENIE BEZPIECZEŃSTWA DANYCH oznacza jakiekolwiek zdarzenie mające wpływ na poufność, integralność lub dostępność Danych Osobowych, takie jak nieupoważnione korzystanie lub ujawnienie Danych Osobowych lub nieupoważniony dostęp do Danych Osobowych, które to zdarzenie narusza prywatność lub bezpieczeństwo Danych Osobowych.
Osoba będąca na utrzymaniu	OSOBA BĘDĄCA NA UTRZYMANIU oznacza małżonka, partnera, dziecko lub beneficjenta Pracownika lub osobę do kontaktu w nagłym wypadku danego Pracownika lub Pracownika Tymczasowego.
Zbyty Podmiot	ZBYTY PODMIOT oznacza Spółkę Grupy, która nie jest już własnością ADP w następstwie zbycia akcji i/lub aktywów spółki lub innej formy zbycia, w związku z czym spółka ta nie może już być uznawana za Spółkę Grupy.
EOG	EOG lub EUROPEJSKI OBSZAR GOSPODARCZY oznacza wszystkie Państwa Członkowskie Unii Europejskiej oraz Norwegię, Islandię i Liechtenstein oraz, na potrzeby Kodeksów, Szwajcarię oraz w Wielkiej Brytanii po jej wystąpieniu ze struktur Unii Europejskiej. Decyzją General Counsel – do opublikowania na stronie www.adp.com - może obejmować inne kraje, których przepisy dotyczące ochrony danych przewidują ograniczenia przekazywania danych podobne do Ograniczeń Przekazywania Danych w EOG.

Obowiązujące Przepisy w EOG	OBOWIĄZUJĄCE PRZEPISY EOG oznaczają wymogi wynikające z Obowiązujących Przepisów EOG, które mają zastosowanie do Danych Osobowych pierwotnie gromadzonych w kontekście działalności Spółki Grupy utworzonej w EOG (również po przekazaniu ich do innej Spółki Grupy utworzonej poza terytorium EOG).
Ograniczenie Przekazywania Danych w EOG	OGRANICZENIE PRZEKAZYWANIA DANYCH W EOG oznacza jakiekolwiek ograniczenie w zakresie transgranicznych transferów Danych Osobowych zgodnie z przepisami ochrony danych danego kraju EOG.
Data Wejścia w Życie	DATA WEJŚCIA W ŻYCIE oznacza datę, w której Kodeksy wchodzą w życie zgodnie z postanowieniami artykułu 1 Kodeksów.
General Counsel	GENERAL COUNSEL oznacza General Counsela spółki Automatic Data Processing, Inc.
Global Chief Privacy Officer	GLOBAL CHIEF PRIVACY OFFICER oznacza Pracownika ADP sprawującego tę funkcję w spółce Automatic Data Processing, Inc.
Spółka Grupy	SPÓŁKA GRUPY oznacza jakikolwiek podmiot prawny będący spółką powiązaną Automatic Data Processing, Inc. i/lub ADP, Inc., jeżeli Automatic Data Processing, Inc. lub ADP, Inc. bezpośrednio lub pośrednio posiada ponad 50% wyemitowanego kapitału zakładowego, posiada co najmniej 50% praw głosu na walnym zgromadzeniu akcjonariuszy/wspólników, posiada prawo do powoływania większości członków zarządu lub w inny sposób kieruje działalnością takiego podmiotu prawnego.
Osoba Fizyczna	OSOBA FIZYCZNA oznacza zidentyfikowaną lub możliwą do zidentyfikowania osobę fizyczną, której Dane Osobowe są Przetwarzane przez ADP działającą w charakterze Przetwarzającego Dane lub Administratora Danych, z wyjątkiem Osób Współzatrudnionych. UWAGA: ADP Privacy Code for Business Data i ADP Workplace Privacy Code nie mają zatem zastosowania do Przetwarzania Danych Osobowych Osób Współzatrudnionych.
Wewnętrzny Przetwarzający	WEWNĘTRZNY PRZETWARZAJĄCY oznacza jakąkolwiek Spółkę Grupy, która Przetwarza Dane Osobowe w imieniu innej Spółki Grupy będącej Administratorem Danych.
Wiodący OOD	WIODĄCY OOD oznacza holenderski Organ Ochrony Danych.
Wymogi Obowiązkowe	WYMOGI OBOWIĄZKOWE oznaczają zobowiązania wynikające z jakichkolwiek Obowiązujących Przepisów dotyczących Przetwarzających Dane, które wymagają Przetwarzania Danych Osobowych w celach związanych z (i) bezpieczeństwem narodowym lub obroną narodową; (ii) bezpieczeństwem publicznym; (iii) zapobieganiem, prowadzeniem śledztw, wykrywaniem i ściganiem przestępstw lub naruszeń zasad etyki zawodów regulowanych; lub (iv) ochroną jakichkolwiek Osób Fizycznych lub praw i wolności Osób Fizycznych.
Global Data Privacy and Governance Team	GLOBAL DATA PRIVACY & GOVERNANCE TEAM oznacza Office of Privacy and Data Governance ADP. Na czele Office of Privacy and Data Governance stoi Global Chief Privacy Officer, a w skład tego Działu wchodzą specjaliści ds. poufności danych, kierownicy ds. poufności danych oraz inni członkowie Personelu będący podwładnymi Global Chief Privacy Officera lub specjalistów

	ds. poufności danych i kierowników ds. poufności danych.
Nadrzędny Interes	NADRZĘDNY INTERES oznacza naglące interesy określone w artykule 13.1 ADP Workplace Privacy Code oraz ADP Privacy Code for Business Data, którym zobowiązania ADP lub prawa Osób Fizycznych określone w artykułach 13.2 i 13.3 Kodeksów mogą, w szczególnych okolicznościach, zostać podporządkowane, jeżeli takie naglące interesy przeważają nad interesami danej Osoby Fizycznej.
Dane Osobowe lub Dane	DANE OSOBOWE lub DANE to wszelkie informacje dotyczące zidentyfikowanej albo możliwej do zidentyfikowania Osoby Fizycznej. Dane Osobowe mogą również dotyczyć danych osobowych zawartych w politykach i normach wdrażających Kodeksy.
Privacy Leadership Council	PRIVACY LEADERSHIP COUNCIL oznacza radę, której przewodniczy Global Chief Privacy Officer, w której skład wchodzą Privacy Stewardzi, członkowie Struktur Poufności wyznaczeni przez Global Chief Privacy Officera oraz inne osoby, których wsparcie może być niezbędne do realizacji założeń Privacy Leadership Council.
Struktury Poufności	STRUKTURY POUFNOŚCI oznaczają członków Global Data Privacy and Governance Team oraz innych członków Działu Prawnego, w tym specjalistów ds. zgodności i inspektorów ochrony danych odpowiadających za zgodność z zasadami prywatności w odpowiednich regionach, krajach, Jednostkach Biznesowych lub obszarach funkcjonalnych.
Privacy Steward	PRIVACY STEWARD oznacza członka kadry kierowniczej ADP, który został powołany przez Odpowiedzialnego Członka Kierownictwa i/lub Wyższe Kierownictwo ADP do wdrożenia i egzekwowania Kodeksów w danej Jednostce Biznesowej ADP.
Przetwarzanie	PRZETWARZANIE oznacza operację lub zestaw operacji wykonywanych na Danych Osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie przechowywanie, organizowanie, modyfikowanie, wykorzystywanie, ujawnianie (w tym udzielanie zdalnego dostępu), przesyłanie i usuwanie Danych Osobowych.
Umowa z Przetwarzającym	UMOWA Z PRZETWARZAJĄCYM oznacza jakąkolwiek umowę dotyczącą Przetwarzania Danych Osobowych zawartą pomiędzy ADP a Zewnętrznym Przetwarzającym.
Specjalista	SPECJALISTA oznacza jakąkolwiek osobę fizyczną (poza pracownikiem) bezpośrednio kontaktującą się z ADP w relacjach zawodowych lub biznesowych. Przykładowo, do grona Specjalistów należą członkowie działu kadr Klienta, którzy kontaktują się z ADP jako użytkownicy produktów lub usług ADP. Do grona Specjalistów zalicza się również przedstawicieli ds. obsługi Klienta, Dostawcy i Kontrahenta, przedstawicieli biznesu, organizacji branżowych, mediów oraz inne osoby, z którymi ADP kontaktuje się w relacjach handlowych.
Odpowiedzialny Członek	ODPOWIEDZIALNY CZŁONEK KIEROWNICTWA oznacza Dyrektora Zarządzającego Spółki Grupy lub kierownika jednostki biznesowej lub obszaru funkcjonalnego, który jest główną osobą zarządzającą budżetem tej Spółki

Kierownictwa	Grupy, jednostki biznesowej lub obszaru funkcjonalnego.
Cel Drugorzędny	CEL DRUGORZĘDNY oznacza jakikolwiek cel poza Celem Pierwotnym, w którym Dane Osobowe ulegają dalszemu Przetwarzaniu.
Umowa o Świadczenie Usług	UMOWA O ŚWIADCZENIE USŁUG oznacza jakikolwiek kontrakt, umowę lub warunki, zgodnie z którymi ADP świadczy na rzecz jakiegokolwiek Klienta Usługi dla Klientów.
Szczególne Kategorie Danych	SZCZEGÓLNE KATEGORIE DANYCH oznaczają Dane Osobowe dotyczące Osoby Fizycznej, które ujawniają jej pochodzenie rasowe albo etniczne, poglądy polityczne lub przynależność do partii politycznych lub innych podobnych organizacji, przekonania religijne albo światopoglądowe, przynależność do związków branżowych lub zawodowych, stan zdrowia fizycznego lub psychicznego, w tym jakiekolwiek opinie w tej sprawie, niepełnosprawność, kod genetyczny, uzależnienia, życie seksualne, popełnione wykroczenia i przestępstwa, wyciąg z rejestru karnego lub postępowania dotyczące zachowań przestępczych lub nielegalnych.
Personel	PERSONEL oznacza łącznie aktualnie zatrudnionych w ADP pracowników oraz Pracowników Tymczasowych obecnie pracujących w ADP.
Umowa z Podprzetwarzającym	UMOWA Z PODPRZETWARZAJĄCYM oznacza umowę w formie pisemnej lub elektronicznej zawartą pomiędzy ADP a Zewnętrznym Podprzetwarzającym zgodnie z artykułem 7.1 Privacy Code dla celów świadczenia Usług Przetwarzania Danych Klienta.
Podprzetwarzający	PODPRZETWARZAJĄCY oznacza, łącznie, Podprzetwarzających ADP oraz Zewnętrznych Podprzetwarzających.
Dostawca	DOSTAWCA oznacza jakąkolwiek Osobę Trzecią dostarczającą towary lub usługi na rzecz ADP (np. usługodawcę, agenta, Przetwarzającego Dane, konsultanta lub sprzedawcę).
Osoba Trzecia	OSOBA TRZECIA oznacza jakąkolwiek osobę, organizację niepubliczną lub organ administracji publicznej niebędący Spółką Grupy.
Zewnętrzny Administrator	ZEWNĘTRZNY ADMINISTRATOR oznacza Osobę Trzecią, która Przetwarza Dane Osobowe i określa cele i sposoby Przetwarzania.
Zewnętrzny Przetwarzający	ZEWNĘTRZNY PRZETWARZAJĄCY oznacza Osobę Trzecią Przetwarzającą Dane Osobowe w imieniu ADP, która nie podlega bezpośrednio ADP.
Zewnętrzny Podprzetwarzający	ZEWNĘTRZNY PODPRZETWARZAJĄCY oznacza jakąkolwiek Osobę Trzecią zaangażowaną przez ADP do działania w charakterze Podprzetwarzającego.

ZAŁĄCZNIK NR 2 – Środki bezpieczeństwa

Autor:	**ADP – Organizacja Bezpieczeństwa Globalnego**
Wersja:	**2.0**
Data publikacji:	**Wrzesień 2019**

Spis treści

Określenia i definicje

Dokument może zawierać następujące określenia:

Określenie lub używany skrót	Definicja
GETS	Global Enterprise Technology & Solutions
GSO	Organizacja Bezpieczeństwa Globalnego (Global Security Organization)
CAB	Zespół zarządzania zmianą (Change Advisory Board)
DRP	Plan przywrócenia gotowości do pracy po wystąpieniu sytuacji nadzwyczajnej
CIRC	Centrum reagowania na krytyczne sytuacje w ramach GSO (Critical Incident Response Center)
SIEM	Zarządzanie bezpieczeństwem informacji oraz wydarzeniami (Security Information and Event Management)
IDS	System wykrywania nieautoryzowanego dostępu (Intrusion Detection System)
DNS	System nazw domen (Domain Name System)
NTP	Protokół synchronizacji czasu (Network Time Protocol)
SOC	Kontrole organizacji usług (Service Organization Controls)
TPSI	Standard Trusted Platform Security Infrastructure

Przegląd

ADP prowadzi formalny program bezpieczeństwa informacyjnego obejmujący administracyjne, techniczne i fizyczne zabezpieczenia chroniące bezpieczeństwo, poufność i integralność informacji klienta. Ten program został zaprojektowany z myślą o (i) zadbaniu o bezpieczeństwo i poufność informacji klienta, (ii) ochronie przed przewidywanymi zagrożeniami dla bezpieczeństwa lub nienaruszalności informacji, a także (iii) ochronie przed nieupoważnionym dostępem lub wykorzystaniem informacji.

Niniejszy dokument zawiera przegląd środków i praktyk ADP odnoszących się do zapewniania bezpieczeństwa informacji, aktualnych na dzień wydania dokumentu, które podlegają zmianie przez ADP. Te wymagania oraz praktyki zostały zaprojektowane z myślą o zachowaniu spójności ze standardami bezpieczeństwa informacji ISO/IEC 27001:2013. ADP okresowo dokonuje oceny swoich polityk i standardów dotyczących bezpieczeństwa. Naszym celem jest zapewnienie, aby program bezpieczeństwa w skuteczny i wydajny sposób zapewniał ochronę wszystkich informacji, które powierzają nam nasi klienci oraz ich pracownicy.

Sekcja 1 – Polityki dotyczące bezpieczeństwa informacji

Niezależność funkcji bezpieczeństwa informacji

Generalny dyrektor ds. bezpieczeństwa w ADP nadzoruje Organizację Bezpieczeństwa Globalnego ADP (GSO) i podlega General Counsel zamiast dyrektorowi ds. informatycznych, co zapewnia GSO potrzebną niezależność od działu IT.. GSO to międzywydziałowy, konwergentny zespół, zajmujący się bezpieczeństwem, który charakteryzuje się multidyscyplinarnym podejściem do zagadnień cyberbezpieczeństwa oraz bezpieczeństwa informatycznego, a także zgodności z przepisami, zarządzania ryzykiem operacyjnym i bezpieczeństwem klienta, ochroną pracowników i odpornością biznesową. Kadra kierownicza GSO, podlegająca naszemu generalnemu dyrektorowi ds. bezpieczeństwa, jest odpowiedzialna za zarządzanie politykami bezpieczeństwa, procedurami oraz wytycznymi.

Formalna definicja Polityki dotyczącej bezpieczeństwa

Firma ADP opracowała i udokumentowała formalne polityki dotyczące bezpieczeństwa, które określają podejście ADP do zarządzania bezpieczeństwem informacji. Konkretne obszary, które zostały objęte tą polityką, to między innymi:

- **Polityka zarządzania bezpieczeństwem** – nakreśla obowiązki Organizacji Bezpieczeństwa Globalnego (GSO) oraz generalnego dyrektora ds. bezpieczeństwa (CSO), w tym obowiązki związane z bezpieczeństwem informacji oraz kontrolę nad procesem rekrutacji z punktu widzenia bezpieczeństwa.
- **Globalna polityka prywatności** – zawiera omówienie kwestii gromadzenia, uzyskiwania dostępu, prawidłowości i ujawniania danych osobowych oraz oświadczenia o ochronie prywatności dla klientów.
- **Polityka dotycząca dopuszczalnego stosowania środków komunikacji elektronicznej oraz ochrony danych pracowników** – zawiera omówienie dopuszczalnego stosowania różnych środków komunikacji elektronicznej, szyfrowania i zarządzania kluczami.
- **Polityka dotycząca przetwarzania danych** – wyznacza wymogi w zakresie klasyfikacji informacji ADP i obejmuje ustanowienie kontroli w zakresie ochrony danych.
- **Polityka dotycząca bezpieczeństwa fizycznego** – definiuje wymagania dotyczące bezpieczeństwa odnoszące się do obiektów ADP oraz pracujących w nich pracowników i gości.
- **Polityka dotycząca zarządzania operacjami w zakresie bezpieczeństwa** – zapewnia minimalną kontrolę w zakresie poprawek systemu, skuteczne reagowanie na zagrożenia ze strony złośliwego oprogramowania, pozwala na przeprowadzanie kontroli kopii zapasowych oraz dbanie o bezpieczeństwo baz danych.
- **Polityka dotycząca monitorowania bezpieczeństwa** – zapewnia kontrolę systemów wykrywania nieautoryzowanego dostępu (IDS), dzienników oraz ochrony przed utratą danych (DLP).
- **Polityka dotycząca dochodzeń oraz zarządzania zdarzeniami** – określa standardy reakcji na zdarzenie, odnajdywania materiałów elektronicznych, ochronę siły roboczej, dostęp do informacji pracowników przechowywanych w formie elektronicznej.
- **Polityka dotycząca dostępu i uwierzytelniania** – wyznacza wymagania dotyczące uwierzytelniania (np. identyfikatora użytkownika i hasła), dostępu zdalnego i bezprzewodowego.
- **Polityka dotycząca bezpieczeństwa sieci** – struktura bezpieczeństwa routerów, zapór sieciowych, AD, DNS, serwerów poczty elektronicznej, DMZ, usług w chmurze, urządzeń sieciowych, serwerów proxy sieci Web oraz przełączników sieciowych.
- **Globalna polityka dotycząca ryzyka strony trzeciej oraz fuzji i przejęć** – ustala minimalny poziomu kontroli bezpieczeństwa w zakresie zatrudniania stron trzecich do wsparcia ADP w realizacji celów biznesowych.

- **Polityka dotycząca zarządzania aplikacjami** – ustanawia odpowiednią kontrolę bezpieczeństwa na każdym etapie rozwoju systemu.
- **Polityka dotycząca odporności biznesowej** –obejmuje ochronę, integralność i utrzymanie ADP przez ustanawianie minimalnych wymogów w zakresie dokumentowania, wdrażania i ciągłego doskonalenia programów odporności biznesowej.
- **Zintegrowana polityka dotycząca zarządzania ryzykiem –** pozwala na identyfikację, monitorowanie, reagowanie, analizę, zarządzanie oraz podejmowanie nowych inicjatyw biznesowych.

Polityki są publikowane w intranecie ADP oraz dostępne dla wszystkich pracowników i kontrahentów w ramach sieci ADP.

Przegląd polityki dotyczącej bezpieczeństwa informacji

ADP dokonuje przeglądu swoich polityk dotyczących bezpieczeństwa informacji przynajmniej raz w roku lub zawsze, kiedy mają miejsce znaczące zmiany, wpływające na funkcjonowanie systemów informatycznych ADP.

Sekcja 2 – Organizacja bezpieczeństwa informacji

Role i obowiązki w zakresie bezpieczeństwa informacji

GSO składa się z międzywydziałowych zespołów zajmujących się bezpieczeństwem, które charakteryzują się multidyscyplinarnym podejściem do zagadnień zgodności z przepisami cyberbezpieczeństwa oraz bezpieczeństwa informatycznego, a także standardów bezpieczeństwa informacji, zarządzania ryzykiem operacyjnym i bezpieczeństwem klienta, ochroną pracowników i odpornością biznesową. Dla wszystkich członków GSO formalnie zdefiniowano role i obowiązki. GSO jest odpowiedzialna za projektowanie, wdrażanie oraz nadzór nad naszym programem bezpieczeństwa informacji na podstawie naszych korporacyjnych polityk. Działania GSO są nadzorowane przez Komitet wykonawczy ds. bezpieczeństwa, w którego skład wchodzą generalny dyrektor ds. bezpieczeństwa w ADP, dyrektor generalny, dyrektor finansowy, dyrektor strategiczny, dyrektor HR oraz główny radca prawny.

Polityka dotycząca mobilnego przetwarzania danych oraz telepracy

ADP wymaga, aby wszystkie poufne informacje były szyfrowane na urządzeniach mobilnych, co umożliwia zapobieganie ich ujawnieniu, które mogłoby wynikać z kradzieży lub utraty komputera/urządzenia. Zaawansowana ochrona w punkcie końcowym oraz uwierzytelnianie dwuskładnikowe poprzez VPN są również wymagane, aby uzyskać zdalny dostęp do sieci korporacyjnych. Wszystkie urządzenia zdalne muszą być chronione hasłem. Pracownicy ADP muszą natychmiast zgłaszać utratę lub kradzież zdalnych urządzeń przetwarzających dane poprzez proces zgłaszania zdarzeń zagrażających bezpieczeństwu danych.

Wszyscy pracownicy oraz kontrahenci, w ramach warunku zatrudnienia w ADP, muszą przestrzegać polityki dotyczącej dopuszczalnego stosowania środków komunikacji elektronicznej oraz ochrony danych, a także innych odpowiednich polityk.

Sekcja 3 – Bezpieczeństwo zasobów ludzkich

Kontrole

Zgodnie z obowiązującymi przepisami prawa w danej jurysdykcji ADP przeprowadza odpowiednie kontrole, proporcjonalnie do obowiązków i odpowiedzialności swoich pracowników, kontrahentów i stron trzecich. Tego typu kontrole potwierdzają, że kandydatowi można powierzyć informacje klienta przed zatrudnieniem jako pracownika.

Kontrola może obejmować następujące elementy:

- Tożsamość/weryfikację zdolności do podjęcia pracy
- Historię zatrudnienia
- Wykształcenie oraz kwalifikacje zawodowe
- Przeszłość kryminalną (o ile zostanie to prawnie umożliwione i w zależności od lokalnych regulacji danego kraju)

Umowy o poufności z pracownikami oraz kontrahentami

Umowy zatrudnienia przez ADP oraz umowy z kontrahentami zawierają warunki określające obowiązki powiązane z informacjami klienta, do których pracownik zyska dostęp. Wszyscy pracownicy ADP oraz kontrahenci są objęci obowiązkami w zakresie zachowania poufności.

Program szkoleniowy z zakresu bezpieczeństwa informacyjnego

Wszyscy pracownicy muszą ukończyć program szkoleniowy z zakresu bezpieczeństwa informacyjnego w ramach swojego planu wdrażania do pracy w firmie. Dodatkowo ADP zapewnia roczne szkolenia z zakresu bezpieczeństwa, aby przypominać pracownikom o ich obowiązkach podczas realizacji codziennych zadań.

Obowiązki pracowników oraz procesy dyscyplinarne

Firma ADP opublikowała politykę dotyczącą bezpieczeństwa, której muszą przestrzegać wszyscy pracownicy. Naruszenia polityk bezpieczeństwa mogą prowadzić do cofnięcia dostępu i/lub podjęcia działań dyscyplinarnych, włącznie z rozwiązaniem umów konsultacyjnych lub stosunku pracy.

Obowiązki w razie zakończenia stosunku pracy

Obowiązki w razie zakończenia stosunku pracy zostały formalnie udokumentowane i obejmują przynajmniej:

- Zwrot wszystkich informacji ADP oraz aktywów znajdujących się w posiadaniu danego pracownika niezależnie od tego, na jakim nośniku są przechowywane
- Anulowanie praw dostępu do obiektów ADP, informacji oraz systemów
- Zmianę haseł do pozostałych, aktywnych i dzielonych z innymi kont, jeśli dotyczy to danej sytuacji
- Transfer wiedzy, jeśli dotyczy to danej sytuacji.

Sekcja 4 – Zarządzanie aktywami

Akceptowalne korzystanie z aktywów

Akceptowalne korzystanie z aktywów zostało wyjaśnione w kilku politykach, mających zastosowanie dla pracowników ADP i kontrahentów, aby informacje ADP i klientów nie były ujawniane w wyniku korzystania z takich aktywów. Przykłady obszarów opisanych w tych politykach: wykorzystanie środków komunikacji elektronicznej, wykorzystanie sprzętu elektronicznego oraz wykorzystanie aktywów informatycznych.

Poufność informacji

Informacjom uzyskanym, utworzonym lub przechowywanym przez lub w imieniu ADP są przypisane następujące klasy poufności (jeśli dotyczy to danej sytuacji):

- Informacje publiczne – przykład: Broszury marketingowe, opublikowane roczne raporty
- Wyłącznie do użytku wewnętrznego ADP – przykład: Komunikacja wewnątrzfirmowa, procedury operacyjne
- Informacje poufne ADP – przykład: Dane osobowe oraz wrażliwe dane osobowe
- Zastrzeżone informacje ADP – przykład: Prognozy finansowe, informacje dotyczące planów strategicznych

Wymagania dotyczące obsługi informacji są bezpośrednio powiązane z klasyfikacją bezpieczeństwa informacji. Dane osobowe oraz wrażliwe dane osobowe są zawsze uznawane za informacje poufne ADP. Wszystkie informacje klienta są klasyfikowane jako poufne.

Pracownicy ADP są odpowiedzialni za ochronę i obsługę informacji zgodnie z ich poziomem klasyfikacji bezpieczeństwa, co zapewnia odpowiednie zabezpieczenie informacji oraz pozwala spełniać właściwe wymogi w zakresie ich obsługi dla każdego poziomu. Klasyfikacja poufności ADP jest stosowana w przypadku wszystkich informacji przechowywanych, przesyłanych lub obsługiwanych przez strony trzecie.

Usuwanie sprzętu i nośników

Kiedy sprzęt ADP, dokumenty, pliki oraz nośniki są usuwane lub ponownie wykorzystywane, należy podjąć odpowiednie środki pozwalające zapobiec odzyskaniu informacji klienta, które były w danym miejscu początkowo przechowywane. Wszystkie informacje przechowywane na komputerach lub elektronicznych nośnikach, niezależnie od klasyfikacji, są w bezpieczny sposób usuwane, chyba że nośnik zostanie fizycznie zniszczony przed wyniesieniem z obiektów ADP lub przekazaniem do ponownego użytku. Procedury bezpiecznego niszczenia/wymazywania informacji ADP przechowywanych na sprzęcie, w dokumentach, plikach oraz na nośnikach zostały formalnie udokumentowane.

Transport fizycznych nośników

Wdrożono organizacyjne środki bezpieczeństwa, które mają na celu ochronę drukowanych materiałów zawierających informacje klienta przed kradzieżą, utratą i/lub nieupoważnionym dostępem/modyfikacją (i) w trakcie przenoszenia, np. w zapieczętowanych kopertach, kontenerach lub podczas osobistego dostarczania do autoryzowanego użytkownika, oraz (ii) w trakcie przeglądania, sprawdzania lub innych procesów, w ramach których są one przenoszone z bezpiecznego miejsca przechowywania.

Sekcja 5 – Kontrola dostępu

Wymagania biznesowe związane z kontrolą dostępu

Polityka kontroli dostępu ADP bazuje na wymaganiach biznesowych. Polityki i standardy kontroli zostały wyrażone w ramach środków kontroli dostępu, które są wdrażane w przypadku wszystkich elementów świadczonej usługi i bazują na zasadach „jak najmniejszych uprawnień" oraz „ograniczonego dostępu".

Dostęp do infrastruktury – zarządzanie kontrolą dostępu

Wnioski o dostęp do przenoszenia, dodawania, tworzenia oraz usuwania są rejestrowane, zatwierdzane i okresowo kontrolowane.

Przynajmniej raz do roku przeprowadzana jest formalna kontrola, aby potwierdzić, że indywidualni użytkownicy spełniają wymagania odnoszące się do danej roli biznesowej i nie będą posiadać dostępu po zmianie stanowiska. Proces jest kontrolowany i dokumentowany w raporcie SOC1[1] typu II. W ramach systemu zarządzania tożsamością wyznaczony zespół ADP jest odpowiedzialny za przyznawanie, odrzucanie, anulowanie, rozwiązywanie, wycofywanie/dezaktywowanie dostępu do obiektów oraz systemów informatycznych ADP. ADP korzysta ze scentralizowanego systemu zarządzania tożsamością i dostępem (IAM), który stanowi narzędzie zarządzane centralnie przez wyznaczony do tego zespół GETS. Zgodnie z prawami dostępu, o które zawnioskowano poprzez scentralizowane narzędzie IAM, uruchomiony zostanie proces zatwierdzania, który może obejmować przełożonego użytkowników. Dostęp jest przyznawany tymczasowo, a dodatkowo istnieją procesy, które zapobiegają przyznaniu takiego dostępu na okres stały. Dostęp użytkownika do obiektu jest natychmiast cofany po ostatnim dniu zatrudnienia poprzez dezaktywację jego karty dostępu (karty pracownika). Identyfikator użytkownika, który było przypisany do danego pracownika, jest natychmiast dezaktywowany. Wszelkie aktywa pracownika są zwracane i sprawdzane przez kompetentnego kierownika liniowego oraz porównywane w stosunku do aktywów znajdujących się na liście w bazie danych. W razie zmiany stanowiska lub zmian organizacyjnych profile użytkownika lub prawa dostępu użytkownika muszą zostać zmienione przez odpowiednie kierownictwo jednostki biznesowej oraz zespół IAM. Dodatkowo co roku przeprowadzana jest formalna kontrola praw dostępu, która ma na celu weryfikację, czy prawa dostępu użytkownika odpowiadają jego roli biznesowej oraz czy nie ma pozostałych nieodpowiednich praw dostępu po zmianie stanowiska.

Polityka dotycząca haseł

Polityki dotyczące haseł pracowników ADP odnoszą się do serwerów, baz danych oraz urządzeń sieciowych i aplikacji, w zakresie, w którym dane urządzenie / dana aplikacja na to pozwalają. Złożoność hasła wynika z analizy ryzyka odnoszącej się do chronionych danych i treści. Te polityki odnoszą się do istniejących standardów branżowych w zakresie siły i złożoności hasła, w tym między innymi uwierzytelniania progresywnego, dwuskładnikowego lub biometrycznego, tam gdzie jest to odpowiednie.

Wymagania dotyczące autoryzacji aplikacji klienta różnią się w zależności od produktu, a usługi (SAML 2.0) są dostępne w określonych aplikacjach ADP, korzystających z ujednoliconej sieci i poziomów zabezpieczeń zarządzanych przez GETS.

[1] W razie określonych usług US Services oferowanych przez ADP są one kontrolowane w ramach raportu SOC 2 typu 2.

Wygaśnięcie sesji

Firma ADP wprowadziła automatyczne wygaśnięcia dla wszystkich serwerów, stacji roboczych, aplikacji i połączeń VPN na podstawie podejścia bazującego na ryzyku, które jest zgodne ze standardami branżowymi. Przywrócenie sesji powinno nastąpić po podaniu przez użytkownika prawidłowego hasła.

Sekcja 6 – Kryptografia

Kontrola kryptograficzna

ADP wymaga, aby informacje wrażliwe wymieniane pomiędzy ADP oraz stronami trzecimi były szyfrowane (lub aby szyfrowany był ich kanał przesyłania) za pomocą akceptowanych w branży technik szyfrowania oraz przy zachowaniu odpowiedniej ich siły. Alternatywnie można używać również prywatnej linii.

Zarządzanie kluczami

ADP posiada wewnętrzny standard bezpieczeństwa szyfrowania, który obejmuje dobrze zdefiniowane zarządzanie kluczami oraz procedury przechowywania kluczy, w tym zarządzanie zarówno symetrycznymi, jak i asymetrycznymi kluczami.

Klucze szyfrowania używane w przypadku informacji ADP są zawsze klasyfikowane jako informacje poufne. Dostęp do takich kluczy jest ściśle ograniczony do osób, które muszą je znać, oraz warunkowany uzyskaniem zgody. Klucze szyfrowania oraz zarządzanie cyklem życia kluczy podlega praktykom odnoszącym się do standardów branżowych.

Sekcja 7 – bezpieczeństwo fizyczne i środowiskowe

Podejście ADP do bezpieczeństwa fizycznego ma dwa cele – stworzenie bezpiecznego środowiska pracy dla pracowników ADP oraz ochronę danych osobowych przechowywanych w centrach danych ADP i innych strategicznych lokalizacjach ADP.

Polityka bezpieczeństwa ADP wymaga, aby kierownictwo ADP identyfikowało obszary wymagające określonego poziomu bezpieczeństwa fizycznego. Dostęp do tych obszarów jest przyznawany tylko uprawnionym pracownikom w określonych celach. Zabezpieczone obszary ADP obejmują różne fizyczne środki bezpieczeństwa, w tym systemy monitoringu wizyjnego, wykorzystanie kart bezpieczeństwa (dostęp na podstawie kontroli tożsamości) oraz ochroniarzy czuwających przy wejściach do obiektów. Odwiedzający mogą uzyskać dostęp tylko pod warunkiem uzyskania upoważnienia i stałego nadzoru.

Sekcja 8 – Bezpieczeństwo operacji

Formalizacja procedur operacji IT

GETS to jednostka ADP odpowiedzialna za operacje w ramach infrastruktury IT oraz konserwację. GETS formalnie utrzymuje i dokumentuje polityki i procedury odnoszące się do operacji IT. Procedury te obejmują między innymi:

- Zarządzanie zmianą
- Zarządzanie kopiami zapasowymi
- Obsługę błędów systemu
- Ponowne uruchamianie i odzyskiwanie systemu
- Monitorowanie systemu
- Tworzenie harmonogramów pracy i monitorowanie

Zarządzanie zmianą infrastruktury

Zespół zarządzania zmianą (CAB), obejmujący reprezentantów z różnych zespołów ADP, jest okresowo zwoływany przez GETS. Podczas spotkań CAB dyskutuje się na temat wpływu okienek wdrażania i przejścia do produkcji, jak również koordynuje się inne zmiany w infrastrukturze produkcyjnej.

Planowanie wydajności systemu oraz akceptacja

Wymagania dotyczące wydajności są stale monitorowane i regularnie kontrolowane. W następstwie tych kontroli zmieniana jest skala systemów oraz sieci. Jeśli trzeba dokonać istotnych zmiany w związku ze zmianą pojemności lub ewolucją technologiczną, zespół GETS zajmujący się analizą może przeprowadzić test danej aplikacji i/lub systemu. W efekcie takiego testu zespół dostarcza szczegółowy raport zmian wydajności poprzez pomiar zmian w (i) komponentach, (ii) konfiguracji systemu lub wersji, (iii) konfiguracji oprogramowania specjalistycznego lub wersji.

Ochrona przed złośliwym kodem

Technologie ochrony punktów końcowych, spełniające branżowe standardy, są wykorzystywane w celu ochrony aktywów ADP zgodnie z najlepszymi praktykami w zakresie standardów branżowych.

Polityka zarządzania kopiami zapasowymi

ADP stosuje polityki, które wymagają tworzenia kopii zapasowych informacji produkcyjnych przez wszystkie działy operacyjne zajmujące się produkcją. Zakres oraz częstotliwość tworzenia kopii zapasowych są wyznaczane zgodnie z wymogami biznesowymi odpowiednich usług ADP, wymogami bezpieczeństwa w odniesieniu do zawartych informacji oraz istotnością informacji w stosunku do odzyskiwania danych w razie ich utraty. Monitorowanie zaplanowanych kopii zapasowych jest przeprowadzane przez GETS w celu identyfikacji problemów lub wyjątków.

Zapisywanie informacji dotyczących bezpieczeństwa oraz monitorowanie

Firma ADP wdrożyła scentralizowaną oraz przystosowaną jedynie do odczytu infrastrukturę rejestracji informacji (SIEM) oraz system korelacji dziennika i powiadamiania (TPSI). Alerty dziennika są monitorowane i obsługiwane na czas przez CIRC.

Wszystkie te systemy są synchronizowane za pomocą unikalnego protokołu Network Time Protocol (NTP) na podstawie referencyjnego zegara.

Każdy indywidualny dziennik zawiera przynajmniej następujące informacje:

- Sygnatura czasowa
- Kto (tożsamość operatora lub administratora)

- Co (informacje na temat wydarzenia)

Ścieżki audytu i wpisy systemu dla aplikacji ADP są zaprojektowane i skonfigurowane z myślą o śledzeniu następujących informacji:

- Autoryzowany dostęp
- Operacje uprzywilejowane
- Nieautoryzowane próby dostępu
- Alerty systemowe lub błędy
- Zmiany w ustawieniach bezpieczeństwa systemu, kiedy system pozwala na takie rejestrowanie

Takie dzienniki są dostępne jedynie dla autoryzowanego personelu ADP i są wysyłane w trybie na żywo w celu zapobiegania naruszaniu danych, zanim zostaną one zapisane na bezpiecznych urządzeniach rejestrujących.

Systemy infrastruktury i monitorowanie

ADP korzysta z odpowiednich środków w celu zapewniania monitorowania infrastruktury przez 24 godziny na dobę i 7 dni w tygodniu. Alerty są obsługiwane przez różne zespoły w zależności od ich poziomu oraz umiejętności potrzebnych do rozwiązania danego problemu.

Obiekty centrum hostującego ADP wykorzystują aplikacje monitorujące, które są stale uruchomione we wszystkich powiązanych systemach przetwarzania oraz w komponentach sieci w celu zapewniania zespołowi ADP proaktywnych powiadomień i ostrzeżeń odnoszących się do przewidywanych problemów.

Zarządzanie podatnością techniczną na zagrożenia

Wszystkie komputery zainstalowane w ramach infrastruktury hostującej muszą być zgodne z instalacją wyspecjalizowanego, zabezpieczonego systemu operacyjnego (lub bezpiecznego procesu budowy). Hostowane operacje obejmują wzmocnioną, zatwierdzoną i ustandaryzowaną konstrukcję dla każdego typu serwera wykorzystywanego w ramach naszej infrastruktury. Niestandardowe instalacje systemów operacyjnych są zabronione, ponieważ mogą tworzyć zagrożenia, takie jak proste hasła do konta systemu, które mogą powodować ryzyko infrastrukturalne. Te konfiguracje zmniejszają ekspozycję hostowanych komputerów, na których działają niepotrzebne usługi, co może prowadzić do zwiększenia zagrożenia.

Firma ADP stosuje udokumentowaną metodologię przeprowadzania okresowych ocen zagrożeń oraz kontroli zgodności aplikacji mających styczność z internetem, a także korespondujących z nimi elementów infrastruktury, co obejmuje przynajmniej 15 podstawowych kategorii testowania. Metodologia ocen bazuje zarówno na wewnętrznych, jak i branżowych najlepszych praktykach, włączając w to między innymi Open Web Application Security Project (OWASP), SANS Institute oraz Web Application Security Consortium (WASC).

Sekcja 9 – Bezpieczeństwo komunikacji

Zarządzanie bezpieczeństwem sieci

ADP korzysta z sieciowych systemów wykrywania nieautoryzowanego dostępu, które monitorują ruch na poziomie infrastruktury sieci (przez 24 godziny na dobę i 7 dni w tygodniu) oraz identyfikują aktywność lub potencjalne ataki.

Wymiana informacji

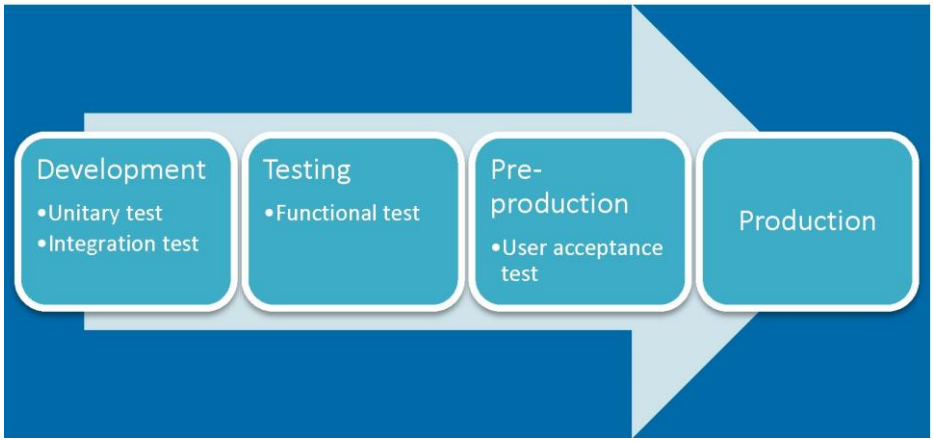
ADP wdraża właściwe środki kontroli, dzięki czemu informacje klientów ADP wysyłane do innych firm są transferowane poprzez autoryzowane systemy i zasoby informatyczne oraz wymieniane jedynie poprzez bezpieczne i autoryzowane mechanizmy transferu ADP.

•

Sekcja 10 – Przejęcie, opracowywanie i konserwacja systemu

Bezpieczeństwo w procesach opracowywania i wsparcia

W trakcie cyklu opracowywania, generowana jest odpowiednia dokumentacja oraz tworzone są plany kontroli dla fazy testów. Różne etapy są określane dla każdego środowiska z odpowiednim zatwierdzeniem na każdym etapie:



- Aby przejść ze środowiska testowania do preprodukcji, wymagana jest zgoda ze strony zespołu ADP ds. jakości.
- Aby przejść z preprodukcji do produkcji, wymagana jest zgoda ze strony zespołu ds. operacji IT.

Od zespołów zajmujących się opracowywaniem rozwiązań wymaga się korzystania z bezpiecznych metod kodowania. Zmiany w aplikacji są testowane w środowiskach opracowywania i regresji, zanim będą mogły wejść do systemu produkcyjnego. Testy są przeprowadzane i dokumentowane. Po zatwierdzeniu zmiany są wprowadzane do produkcji. Testy penetracyjne są przeprowadzane po znaczących zmianach.

Zespół CAB, obejmujący reprezentantów z różnych zespołów ADP, jest okresowo zwoływany przez GETS. Spotkania CAB odbywają się regularnie i mają na celu dyskusję nad wpływami rozmaitych decyzji, uzgadnianie okienek wdrożenia oraz zatwierdzanie realizacji pakietów oprogramowania do produkcji, jak również informowanie na temat innych zmian w infrastrukturze produkcyjnej.

Zespół ds. operacji IT w ADP udziela ostatecznej zgody przed przejściem do środowiska produkcyjnego w zakresie pakietów oprogramowania.

Bezpieczeństwo w środowiskach wdrażania

Środowiska produkcyjne i wdrożeniowe są rozdzielane i wzajemnie od siebie niezależne. Odpowiednia kontrola dostępu jest wykorzystywana do wymuszania właściwego rozdziału obowiązków. Pakiety oprogramowania są dostępne na każdym etapie procesu opracowywania i jedynie dla zespołów zaangażowanych w dany etap.

Dane testowe

W odniesieniu do Polityki ADP dotyczącej zarządzania aplikacjami wykorzystanie prawdziwych, niepoddanych sanityzacji danych w środowiskach opracowywania i testowania jest zabronione, chyba że będzie się to odbywało na wyraźny wniosek i zostanie zatwierdzone przez klienta.

Sekcja 11 – Relacje dostawcy

Identyfikacja ryzyka powiązanego z podmiotami zewnętrznymi

Okresowo wykonywana jest ocena ryzyka stron trzecich, które wymagają dostępu do informacji ADP i/lub klienta, aby skontrolować zgodność stron trzecich z wymogami bezpieczeństwa ADP oraz zidentyfikować luki w stosowanych środkach kontroli. Jeśli uda się zidentyfikować lukę w zakresie bezpieczeństwa, nowe środki kontroli zostaną uzgodnione z podmiotami zewnętrznymi.

Umowy dotyczące bezpieczeństwa informacji z podmiotami zewnętrznymi

ADP zawiera umowy ze wszystkimi stronami trzecimi, które obejmują odpowiednie zobowiązania w zakresie bezpieczeństwa, mające spełniać wymogi bezpieczeństwa ADP.

Sekcja 12 – Zarządzanie zdarzeniami zagrażającymi bezpieczeństwu danych

Zarządzanie zdarzeniami zagrażającymi bezpieczeństwu danych oraz poprawkami

ADP stosuje udokumentowaną metodologię reagowania na zdarzenia zagrażające bezpieczeństwu danych i realizuje tego typu działania na czas, spójnie oraz efektywnie.

W razie wystąpienia zdarzenia wstępnie wyznaczony zespół pracowników ADP realizuje formalny plan reagowania, który dotyczy takich obszarów jak:

- Eskalowanie na podstawie klasyfikacji incydentu lub jego stopnia
- Lista kontaktowa w zakresie zgłaszania/eskalacji wydarzeń
- Wytyczne dotyczące początkowych odpowiedzi oraz kontaktów z zaangażowanymi klientami
- Zgodność z obowiązującymi przepisami dotyczącymi powiadomień o naruszeniu bezpieczeństwa
- Dziennik dochodzenia
- Odzyskiwanie systemu
- Rozwiązywanie, zgłaszanie i sprawdzanie problemów
- Główna przyczyna i środek zaradczy
- Wnioski

Polityka ADP definiuje wydarzenia związane z bezpieczeństwem, sposób zarządzania nim oraz wszystkie obowiązki pracowników dotyczące zgłaszania zdarzeń zagrażających bezpieczeństwu danych. ADP przeprowadza również regularne szkolenia pracowników i kontrahentów, mające na celu dbanie o świadomość dotyczącą wymagań związanych ze zgłaszaniem problemów. Szkolenie jest śledzone, aby zadbać o jego ukończenie.

Sekcja 13 – Aspekty związane z bezpieczeństwem odnoszące się do zarządzania odpornością biznesową

Program odporności biznesowej ADP

ADP dąży do płynnej realizacji usług i działania firmy, dzięki czemu możemy zapewnić naszym klientom najlepsze możliwe usługi. Naszym priorytetem jest identyfikacja – i zmniejszanie zagrożeń technologicznych, środowiskowych, procesowych oraz zdrowotnych, które mogą stanąć na drodze realizacji usług biznesowych. Firma ADP utworzyła zintegrowane ramy, które wyznaczają zasady dotyczące procesów łagodzenia, przygotowywania, odpowiedzi i odzyskiwania danych oraz obejmują:

- Ocenę ryzyka
- Analizę zagrożeń
- Analizę wpływu na działalność biznesową
- Opracowywanie planu
- Planowanie ciągłości działania
- Planowanie przywrócenia gotowości do pracy po wystąpieniu sytuacji nadzwyczajnej
- Planowanie działań w zakresie zdrowia i bezpieczeństwa
- Reakcję w świecie rzeczywistym
- Zarządzanie kryzysowe
- Odpowiedź w sytuacji awaryjnej
- Testowanie i zatwierdzanie
- Kontrolę
- Sprawdzenie
- Wykonanie

Sekcja 14 – Zgodność

Zgodność z politykami i standardami bezpieczeństwa

ADP wdraża procesy pozwalające na wewnętrzne, okresowe przeprowadzanie kontroli zgodności. Dodatkowo ADP okresowo wykonuje audyt SOC1[2] typu II. Tego typu audyt jest realizowany przez dobrze znaną zewnętrzną firmę zajmującą się audytem, a raporty z niego są dostępne co roku dla klientów po złożeniu odpowiedniej prośby (jeśli dotyczy).

Zgodność techniczna

Aby zadbać o zgodność techniczną z najlepszymi praktykami, ADP przeprowadza regularnie zaplanowane kontrole zagrożeń sieci. W efekcie takich kontroli tworzone są priorytety oraz plany działań naprawczych z zespołami hostującymi oraz ich kierownictwem.

Kontrole zagrożeń są realizowane regularnie zarówno w środowiskach wewnętrznych, jak i zewnętrznych. Dodatkowo realizowane są skany kodu źródłowego oraz testy penetracyjne dla każdego produktu. Wykorzystanie wyspecjalizowanych narzędzi do skanowania aplikacji na poziomie ich zagrożeń (jeśli jakieś występują) pozwala na identyfikację i udostępnianie informacji zespołom zajmującym się rozwojem produktu oraz wdrażanie działań naprawczych w procesach zapewniania jakości. Następuje analiza wyników oraz opracowywanie działań korygujących i przypisanie im priorytetów.

Przechowywanie danych

Polityka przechowywania danych ADP odnoszących się do informacji klienta została zaprojektowana z myślą o zachowaniu zgodności z obowiązującymi przepisami prawa. Na koniec umowy z klientem ADP dba o zgodność ze swoimi zobowiązaniami umownymi odnoszącymi się do informacji klienta. ADP zwróci lub zezwoli klientowi na odzyskanie (poprzez pobranie danych) wszystkich informacji klienta wymaganych do kontynuowania przez niego działań biznesowych (jeśli nie zostały wcześniej zapewnione). ADP w bezpieczny sposób zniszczy pozostałe informacje klienta poza sytuacjami wymaganymi przez obowiązujące przepisy, a także z wyjątkiem danych, na których zachowanie klient wyrazi zgodę lub które będą potrzebne w celu rozwiązania sporu.

[2] W sytuacji określonych usług US Services oferowanych przez ADP tworzone są również raporty SOC 2 typu II

ZAŁĄCZNIK NR 3 – Wykaz Spółek Grupy związanych Kodeksem Przetwarzających

ADP (Philippines), Inc	6/F Glorietta 2 Corporate Center, Palm Drive, Ayala Center, Makati City, Filipiny, 1224
ADP (Suisse) SA	Lerzenstr. 10, 8953 Dietikon, Szwajcaria
ADP Brazil Ltda.	João Tibiriçá, 1112 - Vila Anastácio, São Paulo - SP, 05077-000, Brazylia
ADP Canada Co.	3250 Bloor Street West, 16th Floor, Etobicoke, Ontario M8X 2X9, Kanada
ADP Employer Services Belgium BVBA	Koningsstraat 97/4, 1000 Bruksela, Belgia
ADP Employer Services Ceska Republika a.s.	Rohanske nabrezi 670/17, 18600 Praha 8, Czechy
ADP Employer Services GmbH	Frankfurter Str. 227, 63263 Neu-Isenburg, Niemcy
ADP Employer Services Iberia, S.L.U.	Cami Antic de Valencia, 54 B, 08005 Barcelona, Hiszpania
ADP Employer Services Italia SPA	Viale G. Richard 5/A - 20143 Mediolan, Włochy
ADP ES Tunisie SARL	MIRMAR Business City Lot B16 Centre Urbain Nord - 1003 Tunis, Tunezja
ADP Europe, S.A.S.	31, avenue Jules Quentin, 92000 Nanterre, Francja
ADP France SAS	31, avenue Jules Quentin, 92000 Nanterre, Francja
ADP GlobalView B.V.	Lylantse Bann 1,2908 LG Capelle aan den, Ljseel, Holandia
ADP GSI France SAS	31-41, avenue Jules Quentin, 92000 Nanterre, Francja
ADP HR and Payroll Services Ireland Limited	Unit 1, 42 Rosemount Park Dr, Rosemount Business Park, Dublin, D11 KC98, Ireland
ADP India Private Ltd.	Tamarai Tech Park, S.P. Plot No.16 to 20 & 20A, Thiru-Vi-Ka Industrial Estate, Inner Ring Road, Guindy, Chennai - 600 032 Indie
ADP International Services B.V.	Lylantse Bann 1,2908 LG Capelle aan den, Ljseel, Holandia
ADP Nederland B.V.	K.P. van der Mandelelaan 9-35, 3062 MB Rotterdam, Postbus 4065, 3006 AB Rotterdam
ADP Outsourcing Italia SRL	Viale G. Richard 5/A - 20143 Mediolan, Włochy
ADP Payroll Services, Inc.	One ADP Boulevard, Roseland, NJ, USA 07068
ADP Polska Sp. z o.o.	Prosta 70, 00-838 Warszawa
ADP Private Limited	6-3-1091/C/1, Fortune 9, Raj Bhavan Road, Somajiguda, Hyderabad, Telangana, Indie - 500082

ADP RPO UK Limited	22 Chancery Lane, London, Anglia, WC2A 1LS
ADP RPO, LLC	3401 Technology Drive, Findlay, OH, USA 45840
ADP Screening and Selection Services, Inc.	One ADP Boulevard, Roseland, NJ, USA 07068
ADP Slovakia s.r.o.	Cernysevskeho 26, 851 01 Bratysława, Słowacja
ADP Software Solutions Italia SRL	Via Oropa 28 - 10153 Turyn, Włochy
ADP Sverige AB	Östermalmstorg 1, 114 42 Stockholm, Szwecja
ADP, Inc.	One ADP Boulevard, Roseland, NJ, USA 07068
Automatic Data Processing (ADP) Romania SRL	4B Gara Herastrau St., 1st - 6th floor, District 2, Bukareszt, Rumunia 020334
Automatic Data Processing Limited (Australia)	6 Nexus Court, Mulgrave, VIC 3170, Australia
Automatic Data Processing Limited (UK)	Syward Place, Pyrcroft Road, Chertsey, Surrey, KT16 9JT, England
Business Management Software Limited	2 Peterborough Business Park, Lynch Wood, Peterborough, Cambridgeshire, PE2 6FZ, England
Celergo Hungary kft	1093 Budapest, Kozraktar utca 30. 6. emelet., Cg. 01-090980824, Hungary
Celergo LLC	One ADP Boulevard, Roseland, NJ, USA 07068
Celergo PTE. LTD.	62, Ubi Road 1, #11-07, Oxley Bizhub 2, Singapur 408733
Ridgenumber - Processamento de Dados LDA	Rua Brito e Cunha, 254 - 2°, 4450-082 Matosinhos, Portugalia
The Marcus Buckingham Company	8350 Wilshire Boulevard, #200, Beverly Hills, CA, USA 90211
VirtualEdge Corporation	One ADP Boulevard, Roseland, NJ, USA 07068