Nazwa polityki: Polityka ochrony danych RODO
Właściciel: Radosław Bieliński
Zatwierdził: Radosław Bieliński
Data zatwierdzenia: 12.05.2020 r.
Data weryfikacji przez Dyrektora ds. Zgodności (Chief Compliance Officer): 12.05.2020 r.

WERSJA	AUTOR	OPIS ZMIANY	ZATWIERDZIŁ
16.06.2020 r.	Radosław Bieliński	Dostosowanie polityki do standardów dokumentacji Grupowej	Radosław Bieliński

DYWIDAG
SAFER. STRONGER. SMARTER.

Spis treści

1. Wprowadzenie

Prywatność jest prawem fundamentalnym - jej ochrona jest ważna dla naszej organizacji. DYWIDAG jako globalna Grupa, zobowiązuje się więc do przestrzegania wszystkich przepisów, zasad i regulacji związanych z Ochroną danych, której podlegają podmioty powiązane, w tym m.in. Ogólnego Rozporządzenia o Ochronie Danych („RODO").

DYWIDAG gromadzi, przechowuje i przetwarza dane osobowe dotyczące różnych Podmiotów danych, takich jak pracownicy, kandydaci na stanowiska pracy, klienci, dostawcy i inne strony trzecie. Poprawne i zgodne z prawem traktowanie danych osobowych jest prowadzone z zachowaniem poufności i w oparciu o dobre imię Grupy DYWIDAG, jako społecznie odpowiedzialnego partnera biznesowego i pracodawcy.

Niniejsza polityka określa wymogi, do których wszyscy objęci jej zakresem muszą się stosować i zawiera przyjęte na całym świecie zasady dotyczące prywatności danych. Wymogi te obowiązują w odniesieniu do wszystkich spółek powiązanych DYWIDAG, ich pracowników, kontrahentów, pracowników tymczasowych i pracowników agencyjnych - włącznie ze wszystkimi osobami, z którymi współpracujemy lub, którzy występują w naszym imieniu i mogą potrzebować sporadycznego dostępu do danych. Polityka ta obejmuje wszystkie czynności związane z przetwarzaniem dotyczące danych osobowych oraz pomoże Ci rozpoznać, które dane mogą być danymi osobowymi, a także jakie są Twoje prawa i obowiązki w odniesieniu do takich danych.

Polityka ochrony danych DYWIDAG stanowi uzupełnienie krajowych przepisów ochrony danych lub obowiązuje w przypadku braku ustawodawstwa krajowego. Spółki powiązane DYWIDAG, których niniejsza polityka nie obowiązuje w sposób bezpośredni z uwagi na istniejące zasady zarządzania (np. spółki joint venture), muszą wdrożyć swoje własne zasady i procedury w oparciu o swoje krajowe ustawodawstwo i wymogi.

Naruszenie właściwych przepisów dotyczących prywatności danych może spowodować ogromne szkody dla DYWIDAG, w postaci utraty dobrego imienia, poważnych kar oraz wpłynąć na zaufanie ze strony klientów, pracowników i opinii publicznej, jak również wszystkich pozostałych interesariuszy. Dlatego też oczekujemy od Ciebie stosowania się do wymogów określonych w niniejszej Polityce.

2. Zakres

Zakres niniejszej Polityki obejmuje:

- wszystkie czynności związane z przetwarzaniem danych, obejmujące dane osobowe i wrażliwe dane osobowe, w ramach których DYWIDAG występuje jako administrator danych, włącznie
  z danymi osobowymi w formie papierowej, przechowywanymi w archiwum;
- wszystkich Pracowników, Kontrahentów, Strony trzecie Procesorów oraz inne osoby przetwarzające dane osobowe lub wrażliwe dane osobowe w imieniu Grupy DYWIDAG;
- wszystkie terytoria geograficzne, włącznie z Państwami trzecimi poza Unią Europejską (UE). Wszystkie spółki powiązane DYWIDAG oraz ich pracownicy muszą przetwarzać dane osobowe z zachowaniem należytej staranności oraz zgodnie z wymogami ustawowymi i niniejszą polityką.

W szczególności w przypadku Podmiotów i czynności związanych z przetwarzaniem danych, które podlegają RODO, niezbędne są dodatkowe lokalne wytyczne i procedury. Muszą one być opracowywane i ustanawiane przez lokalną kadrę zarządzającą lub wyznaczonego przedstawiciela działu ds. zgodności (Compliance) z zasadami obowiązującymi od maja 2018 r., nie licząc ewentualnego ustawodawstwa krajowego. Spółki powiązane prowadzące działalność poza Unią Europejską muszą również opracować dodatkowe, lokalne zasady i wytyczne, jeśli jest to niezbędne dla zachowania zgodności z ich ustawodawstwem krajowym oraz przepisami o ochronie danych. Spółki powiązane DYWIDAG, których nie dotyczą żadne krajowe przepisy o ochronie danych, muszą przyjąć i stosować niniejszą politykę.

Jeśli odpowiednie ustawodawstwo krajowe koliduje z niniejszą polityką lub zawiera bardziej restrykcyjne wymogi, będzie ono mieć pierwszeństwo. Obowiązkiem lokalnej kadry zarządzającej Podmiotu jest monitorowanie krajowego ustawodawstwa w zakresie ochrony danych oraz jego rozszerzeń lub zmian. Jeżeli zmiany wprowadzone do ustawodawstwa krajowego będą kolidować z niniejszą polityką, należy to zgłosić Dyrektorowi ds. Zgodności (Chief Compliance Officer).

3. Definicje

- **„Dane osobowe”**: wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, tzw. „podmiotu danych”
- **„Podmiot danych”**: możliwa do zidentyfikowania osoba fizyczna to osoba, którą można zidentyfikować, bezpośrednio lub pośrednio, w szczególności w odniesieniu do identyfikatora takiego jak imię, nazwisko, adres, numer identyfikacyjny, wszelkiego rodzaju dane lokalizacyjne, identyfikator online lub jeden, lub więcej czynników właściwych dla fizycznej, fizjologicznej, genetycznej, umysłowej, ekonomicznej, kulturalnej lub społecznej tożsamości tej osoby fizycznej. Informacje dotyczące pochodzenia rasowego lub etnicznego danej osoby, jej opinii politycznych, przekonań religijnych lub tym podobnych, członkostwie w związkach zawodowych, zdrowiu lub stanie fizycznym lub umysłowym, zdrowiu i życiu seksualnym, zarzutach karnych lub popełnionych przestępstwach uznaje się za dane wrażliwe; należą one do specjalnych kategorii danych osobowych. W ramach ustawodawstwa krajowego dalsze kategorie danych mogą być uznawane za wysoce wrażliwe lub też treść kategorii danych może być archiwizowana w inny sposób.

  Dane zanonimizowane oraz dane niezwiązane z osobą fizyczną (np. dane spółki, takie jak nazwy i adresy firm) nie są objęte niniejszą polityką.
- **„Przetwarzanie**”: danych osobowych oznacza wszelkie operacje lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych, w sposób zautomatyzowany lub nie, takie jak gromadzenie, rejestrowanie, organizowanie, strukturyzowanie, przechowywanie, adaptowanie lub przekształcanie, odtwarzanie, konsultowanie, użytkowanie, ujawnianie poprzez transmisję, rozpowszechnianie lub innego rodzaju udostępnianie, zestawianie lub łączenie, ograniczanie, usuwanie lub niszczenie
- **„Administrator danych”**: to „osoba fizyczna lub prawna, organ państwowy, agencja lub inny urząd, który samodzielnie lub wraz z innymi określa cele i sposoby przetwarzania danych osobowych”
- **„Procesorzy danych”**: przetwarzają dane osobowe w imieniu administratora danych (np. agencja ds. płac wynajęta przez DYWIDAG, spółkę będącą administratorem danych, do księgowości płacowej)
- „**Naruszenie bezpieczeństwa”**: to każdy incydent, który skutkuje nieupoważnionym dostępem do danych, aplikacji, serwisów, sieci i/lub urządzeń poprzez obejście ich podstawowych mechanizmów bezpieczeństwa

- Do naruszenia bezpieczeństwa dochodzi, kiedy osoba lub aplikacja w sposób bezprawny wchodzi na prywatny, poufny lub nieautoryzowany logiczny obwód informatyczny. Naruszenie bezpieczeństwa jest również znane jako złamanie zabezpieczeń, a jego konsekwencją może być potencjalnie naruszenie danych osobowych
- **„Naruszenie danych”**: to naruszenie danych prowadzące do przypadkowego lub bezprawnego zniszczenia, utraty, przekształcenia, nieautoryzowanego ujawnienia lub dostępu do danych osobowych przekazywanych, przechowywanych lub w inny sposób przetwarzanych w formie elektronicznej lub drukowanej, skutkujące potencjalnym naruszeniem poufności lub integralności tych danych
- „**Strona trzecia**” oznacza osobę fizyczną lub prawną, organ państwowy, agencję lub urząd inny niż podmiot danych, administrator, procesor i osoby, które, pod bezpośrednim nadzorem administratora lub procesora, są upoważnione do przetwarzania danych osobowych.

4. Ramy i zasady ochrony danych

Niniejsza sekcja opisuje podstawowe ramy i zasady, definiuje minimalne standardy i wymogi naszego systemu ochrony danych oraz zapewnia wytyczne w celu zagwarantowania, monitorowania i utrzymywania odpowiedniego poziomu bezpieczeństwa danych osobowych. W ramach organizacji DYWIDAG dane osobowe są gromadzone w sposób przejrzysty i tylko przy pełnej współpracy i wiedzy stron zainteresowanych. Kiedy już dane osobowe zostaną zgromadzone, stosuje się następujące zasady:

Dane osobowe i wszystkie czynności związane z przetwarzaniem będą

- poprawnie rejestrowane i aktualizowane
- gromadzone wyłącznie w konkretnych, wyraźnych i zgodnych z prawem celach
- przechowywane wyłącznie tak długo, jak to konieczne oraz zgodnie z ustawowymi wymogami dotyczącymi okresów przechowywania danych
- przetwarzane w sposób uczciwy i zgodny z prawem
- chronione przed wszelkim nieupoważnionym lub nielegalnym dostępem oraz niewłaściwym użyciem przez strony wewnętrzne lub zewnętrzne
- odpowiednie, właściwe i ograniczone do tego, co niezbędne.

Dane te nie będą:

- przekazywane na poziomie wewnętrznym bez określonego celu
- przekazywane organizacjom (i podmiotom powiązanym), stanom lub państwom, które nie posiadają odpowiednich zasad i regulacji dotyczących ochrony danych.

Oprócz sposobów przetwarzania danych, każdy podmiot w ramach Grupy DYWIDAG posiada bezpośrednie zobowiązania wobec osób, do których te dane należą. W szczególności na wniosek tych osób musimy udzielić informacji na temat a) danych, które przetwarzamy, b) sposobu przetwarzania tych danych i c) osób, które miały dostęp do tych informacji.

Musimy również:

- posiadać ustalenia na wypadek utraty, uszkodzenia lub naruszenia danych
- zezwolić osobom fizycznym na wnioskowanie o modyfikację, usunięcie, ograniczenie lub poprawienie danych znajdujących się w naszych bazach danych.

W celu zapewnienia odpowiedniego poziomu ochrony danych osobowych zobowiązujemy się do:

- Ograniczenia i monitorowania dostępu do danych osobowych, w szczególności do wrażliwych danych osobowych
- Opracowania przejrzystych procedur gromadzenia danych
- Przeszkolenia pracowników pod kątem prywatności online i środków bezpieczeństwa
- Zbudowania bezpiecznych sieci w celu ochrony danych online przed cyber-atakami
- Ustanowienia jasnych procedur zgłaszania naruszeń prywatności lub niewłaściwego użycia danych
- Za każdym razem, gdy jest to uznawane za niezbędne, dodawania zapisów umownych lub przekazywania oświadczeń w sprawie sposobu, w jaki przetwarzamy dane
- Ustanowienia najlepszych praktyk ochrony danych (kontrola dostępu do budynków, biur i systemów informatycznych, niszczenie dokumentów, bezpieczne zamki, urządzenia i szyfrowanie danych, częste wykonywanie kopii zapasowych, autoryzacja dostępu, plany dotyczące usuwania skutków awarii itp.)

Zasady te opisano bardziej szczegółowo w poniższych sekcjach niniejszej polityki.

4.1 Główne zasady przetwarzania danych osobowych

Podczas przetwarzania danych osobowych obowiązują następujące, możliwe do egzekwowania

zasady:

- **Uczciwość, zgodność z prawem i przejrzystość:** dane osobowe mogą być gromadzone i przetwarzane wyłącznie w konkretnych, wyraźnych i zgodnych z prawem celach, w sposób uczciwy i przejrzysty oraz zgodny z obowiązującym prawem. Podmiot danych musi zostać poinformowany o sposobie przetwarzania jego danych. Ogólnie rzecz biorąc, dane osobowe należy gromadzić bezpośrednio od osoby, której przetwarzanie dotyczy. Podczas gromadzenia danych podmiot danych musi albo mieć świadomość, albo otrzymać informację o a) tożsamości administratora danych b) celu przetwarzania danych i c) stronach trzecich lub kategoriach stron trzecich, którym dane mogą zostać przekazane
- **Ograniczenie celu**: dane osobowe mogą być gromadzone i przetwarzane wyłącznie w celu zdefiniowanym przed ich zgromadzeniem, ograniczonym do czynności niezbędnych w związku z celami, dla których są przetwarzane i nie mogą być następnie przetwarzane w sposób niespójny z tymi celami
- **Minimalizacja danych**: dane osobowe muszą być ograniczone do odpowiedniego, niezbędnego i istotnego zakresu dla osiągnięcia celu ich przetwarzania. Zabrania się gromadzenia danych osobowych z wyprzedzeniem i przechowywania ich do potencjalnych przyszłych celów, o ile Podmiot danych nie wyraził zgody lub nie stanowi to wymogu ustawodawstwa krajowego, lub nie jest przez nie dozwolone
- **Poprawność**: Zarchiwizowane dane osobowe muszą być prawidłowe, kompletne i - jeśli jest konieczne - aktualizowane. Należy podjąć odpowiednie kroki dla zapewnienia, że niedokładne lub niepełne dane będą usuwane, poprawiane, uzupełniane lub aktualizowane
- **Ograniczenie przechowywania i usuwanie:** dane osobowe muszą być przechowywane wyłącznie tak długo, jak jest to wymagane dla osiągnięcia planowanych celów ich gromadzenia i przetwarzania. Po wygaśnięciu okresów prawnych lub związanych z procesami biznesowymi, Dane osobowe, które nie są już potrzebne, należy w bezpieczny sposób usunąć
- **Integralność i poufność, bezpieczeństwo danych:** dane osobowe należy przetwarzać w sposób, który a) zapewnia odpowiednie bezpieczeństwo danych; b) zapewnia bezpieczne przechowywanie danych przy użyciu odpowiednich, nowoczesnych systemów i aktualizowanego oprogramowania.

W celu zapobiegania nieupoważnionemu lub nielegalnemu dostępowi i niewłaściwemu używaniu, przetwarzaniu lub dystrybucji danych, jak również ich przypadkowej utracie, modyfikacji lub zniszczeniu, muszą obowiązywać formalnie opisane przez wszystkie nasze Podmioty, odpowiednie środki bezpieczeństwa technicznego i organizacyjnego (tzw. „TOM” - Technical and Organizational

Measures tj. kontrola dostępu, zasady dotyczące haseł, fizyczne bezpieczeństwo serwerów, wytyczne dotyczące kopii zapasowych itp.).

Stosowanie się do tych zasad musi być poparte rejestrem systemów (informatycznych) i czynności związanych z przetwarzaniem, w którym udokumentowane są wszystkie informacje i procedury dotyczące danych osobowych (np. kategoria podmiotu danych, kategoria Danych osobowych, cel przetwarzania). Wszystkie Podmioty muszą prowadzić tego rodzaju Rejestr czynności związanych z przetwarzaniem, w szczególności Podmioty dokonujące czynności związanych z przetwarzaniem podlegających RODO (art. 30 RODO).

4.2 Zgodność przetwarzania danych z prawem

DYWIDAG musi zagwarantować, że przetwarzanie danych będzie zgodne z prawem i dokumentować zgodne z prawem podstawy przetwarzania. Aby dane osobowe były przetwarzane w sposób zgodny z prawem, muszą one być przetwarzane na podstawie jednej z następujących podstaw prawnych:

- Zgoda podmiotu danych na przetwarzanie (np. od kandydatów na stanowisko pracy przesyłających CV, newsletter z materiałami marketingowymi)
- Przetwarzanie jest niezbędne do zawarcia lub zrealizowania umowy z podmiotem danych (np. umowa o pracę)
- Dla zachowania zgodności z obowiązkiem prawnym, któremu podlegają DYWIDAG i jej spółki powiązane (administratorzy danych) (np. archiwizacja dokumentów ZUS i podatkowych)
- Dla uzasadnionego interesu DYWIDAG lub strony, której dane osobowe są ujawniane (np. pliki dziennika lub adresy IP użytkownika mogą być przechowywane tymczasowo; jest to uzasadnione dla zapewnienia prawidłowego funkcjonowania sieci i bezpieczeństwa)
- Dla kluczowego interesu społeczeństwa i innych interesariuszy
- Dla realizacji zadań i zobowiązań publicznych.

Przetwarzanie specjalnych kategorii danych osobowych musi być wyraźnie dozwolone lub uregulowane przez prawo krajowe. Ponadto przetwarzanie może być dozwolone, jeśli jest to niezbędne dla danego organu do wypełnienia jego praw i obowiązków dotyczących przepisów o zatrudnieniu. Pracownik może również wyraźnie zgodzić się na przetwarzanie danych.

Z wyjątkiem przechowywania danych, przetwarzanie danych zostanie natychmiast zakończone, kiedy

nie będzie już ku temu podstaw prawnych.

4.3 Prawa Podmiotów danych

Na wniosek Podmiotu danych, odpowiedni Podmiot przetwarzający musi go poinformować o zgromadzonych danych osobowych w zakresie obowiązujących przepisów prawa. Ogólnie rzecz biorąc, podmioty danych mogą:

- zażądać dostępu do wszelkich danych osobowych przechowywanych na ich temat przez administratora danych
- uniemożliwiać, sprzeciwiać się lub ograniczać przetwarzanie ich danych osobowych, np. do bezpośrednich celów marketingowych
- prosić o poprawienie nieprawidłowych danych osobowych
- zażądać informacji na temat tożsamości odbiorcy lub kategorii odbiorców, jeśli ich dane osobowe zostały przekazane stronom trzecim (np. procesorom danych będącym podwykonawcami)
- zażądać usunięcia swoich danych, jeśli przetwarzanie tych danych nie ma podstaw prawnych lub jeśli podstawa prawna nie ma już zastosowania. To samo dotyczy sytuacji, w której cel przetwarzania danych wygasł lub nie dotyczy już tych danych z innych powodów. Określone prawem okresy przechowywania danych mogą być nadrzędne w stosunku do tego prawa i należy je ściśle monitorować.

W przypadku otrzymania wniosku o udzielenie dostępu danych od Podmiotu, należy natychmiast skontaktować się z Dyrektorem ds. Zgodności (Chief Compliance Officer). Wniosek taki zostanie zrealizowany tak szybko jak to możliwe, nie przekraczając terminu 30 dni i przekazany Podmiotowi danych w bezpieczny sposób.

4.4 Transfery Danych osobowych oraz Przetwarzanie danych (umownych) w czyimś imieniu

Przekazywanie danych osobowych wewnątrz Grupy lub przetwarzanie danych osobowych „w imieniu” Administratora danych, muszą opierać się wg. zasad podanych w sekcjach od 4.1 do 4.3 i być zgodne z obowiązującymi przepisami i ustawowymi wymogami dotyczącymi ochrony danych danego kraju.

„Przetwarzanie danych w czyimś imieniu” oznacza, że Procesor dokonuje przetwarzania danych osobowych w imieniu i zgodnie z instrukcjami Administratora, który określa cele i środki przetwarzania danych osobowych. Innymi słowy, Procesor jest wynajmowany przez Administratora danych jako Procesor danych w celu przetwarzania danych osobowych (np. outsourcing zarządzania płacami, outsourcing serwerów informatycznych na rzecz dostawcy hostingu/usług w chmurze).

Czynności „przetwarzania w czyimś imieniu” na terenie UE nie będą podlegać outsourcingowi bez wiążącej umowy pisemnej określającej przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych i kategorie Podmiotów danych oraz obowiązki i prawa Podmiotu DYWIDAG występującego jako Administrator (art. 28 RODO UE). W przypadku, jeśli dane osobowe będą przekazywane przez Podmiot DYWIDAG (Administratora danych) na terenie UE odbiorcy (Procesorowi danych) poza UE (włącznie z transferami wewnątrz Grupy), odbiorca musi wyrazić zgodę na utrzymanie poziomu ochrony danych równoważnego z niniejszą Polityką ochrony danych.

Administrator będzie korzystać wyłącznie z usług Procesorów danych zapewniających gwarancje dostateczne do wdrożenia odpowiednich środków technicznych i organizacyjnych, tak aby przetwarzanie spełniało wymogi niniejszej polityki i zapewniało ochronę praw Podmiotu danych.

4.5 Poufność przetwarzania

Wszelkie rodzaje danych osobowych są objęte tajemnicą danych, dlatego też:

- zabrania się wszelkiego nieupoważnionego gromadzenia i przetwarzania takich danych przez pracowników
- zabrania się wszelkiego przetwarzania danych przez pracownika, który nie został do tego upoważniony w ramach swoich uzasadnionych obowiązków.

Zastosowanie ma zasada „niezbędnego minimum”: pracownicy mogą posiadać dostęp do danych osobowych wyłącznie w stopniu odpowiednim do rodzaju i zakresu danego zadania. Wymaga to starannego podziału i oddzielenia oraz wdrożenia ról i zakresów obowiązków.

Zabrania się pracownikom wykorzystywania zgromadzonych danych osobowych do celów prywatnych lub komercyjnych, lub ich ujawniania nieupoważnionym osobom; pracodawcy muszą poinformować

swoich pracowników w momencie powstania stosunku pracy o obowiązku ochrony tajemnicy danych oraz zapoznać ich z niniejszą polityką (np. wymagając potwierdzenia jej na piśmie). Obowiązek ten pozostanie w mocy nawet po ustaniu zatrudnienia.

4.6 Bezpieczeństwo przetwarzania

Dane osobowe należy chronić przed nieupoważnionym dostępem i niezgodnym z prawem przetwarzaniem lub ujawnianiem, jak również przypadkową utratą, modyfikacją lub zniszczeniem. Obowiązuje to niezależnie od tego czy dane są przetwarzane w formie elektronicznej, czy papierowej. Tego rodzaju techniczne i organizacyjne środki bezpieczeństwa muszą opierać się na najnowocześniejszych technologiach, analizie ryzyka związanego z przetwarzaniem danych oraz ochroną danych wrażliwych. Ogólnie rzecz biorąc, zarówno DYWIDAG, jak i każda ze spółek powiązanych musi upewnić się, że:

- budynki i pomieszczenia biurowe są odpowiednio chronione przed nieupoważnionym dostępem (np. systemy alarmowe, mechanizmy kontroli i rejestracji wejścia)
- dane osobowe są przechowywane w sposób bezpieczny, przy użyciu nowoczesnego, aktualizowanego oprogramowania
- dostęp do danych osobowych jest ograniczony wyłącznie do personelu, który potrzebuje takiego dostępu i obowiązują odpowiednie środki bezpieczeństwa w celu zapobiegania nieupoważnionemu udostępnianiu informacji
- dane personelu są przekazywane wyłącznie bezpiecznymi środkami (np. szyfrowanie e-maili/laptopów, szyfrowane urządzenia USB)
- dostęp do danych osobowych jest monitorowany i protokołowany (np. zapisy audytu dotyczące pozycji danych, zapisy dziennika)
- dostępność i odzyskiwanie danych (kopie zapasowe i procedury dotyczące usuwania skutków awarii, firewalle, programy antywirusowe)
- kiedy dane osobowe są usuwane, odbywa się to w sposób bezpieczny, uniemożliwiający cofnięcie usunięcia
- obowiązują odpowiednie mechanizmy kontrolne w przypadku outsourcingu danych osobowych na rzecz zewnętrznego procesora danych
- incydenty dotyczące bezpieczeństwa / naruszenia danych oraz wszelkie inne incydenty są odpowiednie zgłaszane i rozwiązywane.

Środki techniczne i organizacyjne muszą zostać zdefiniowane i wdrożone przed wprowadzeniem nowych metod przetwarzania danych osobowych, w szczególności nowych systemów i aplikacji informatycznych. Muszą one być nieustannie oceniane pod kątem opracowań technicznych i zmian organizacyjnych.

4.7 Świadomość na temat ochrony danych

Skuteczność organizacji ochrony danych DYWIDAG wymaga, aby wszystkie spółki powiązane i wszyscy ich pracownicy, którzy przetwarzają dane osobowe dla DYWIDAG mieli świadomość znaczenia ochrony danych i prywatności danych.

Dlatego też kadra zarządzająca każdego Podmiotu DYWIDAG ma obowiązek promować tę świadomość wśród wszystkich pracowników przetwarzających dane osobowe, np. poprzez regularne, odbywające się co najmniej raz w roku szkolenia z ochrony danych, programy świadomości korporacyjnej i uwrażliwiania, w formie szkoleń online lub za pomocą innych, odpowiednich metod (np. szkoleń na miejscu).

4.8 Struktura organizacyjna

Kadra zarządzająca wszystkich Podmiotów DYWIDAG jest odpowiedzialna za zapewnienie odpowiedniego poziomu ochrony danych, zgodnego ze wszystkimi obowiązującymi przepisami, we wszystkich swoich spółkach powiązanych i umożliwia wdrożenie odpowiedniego systemu ochrony danych.

Dla zapewnienia odpowiedniego poziomu ochrony danych i egzekwowania niniejszej polityki, wymagane jest wdrożenie następujących ról i funkcji:

- Koordynatorzy ochrony danych („DPC” – Data Protection Coordinator), którzy muszą zostać wyznaczeni przez lokalną kadrę zarządzającą każdego Podmiotu. Koordynatorzy ochrony danych są osobami do kontaktu na stronie internetowej w zakresie ochrony danych. Mogą oni przeprowadzać kontrole i muszą informować pracowników o treści niniejszej polityki ochrony danych

- Pełnomocnicy ds. ochrony danych niejawnych („DPO" – Data Protection Officer), tam gdzie jest to wymagane przez obowiązujące prawo.

Krajowe wymogi prawne mogą określać dodatkowe role i zadania. Regionalna i/lub Lokalna kadra kierownicza Podmiotu gwarantuje, że DPO i DPC:

- są wystarczająco zaangażowani, w odpowiednim czasie, we wszystkie kwestie związane z ochroną danych osobowych
- uzyskują dostęp do wszystkich procesów dotyczących przetwarzania danych osobowych
- mogą bezpośrednio podlegać Dyrektorowi ds. Zgodności (Chief Compliance Officer)
- są zobowiązani do zachowania tajemnicy i nieujawniania informacji dotyczących ich czynności, zgodnie z obowiązującymi przepisami prawa.

DPC i DPO mogą też wykonywać inne zadania, obowiązki i funkcje, jeśli nie stanowią one konfliktu interesów z ich obowiązkami jako DPC lub DPO. DPC i DPO mogą być wyznaczani dla kilku Podmiotów regionu lub kraju, jeśli nie stanowi to konfliktu interesów.

4.9 Incydenty związane z ochroną danych

Następujące incydenty związane z ochroną danych muszą być niezwłocznie zgłaszane przez regionalną lub lokalną kadrę kierowniczą Podmiotu do lokalnych DPC i/lub DPO mających stosowne uprawnienia, jak również do Dyrektora ds. Zgodności ((Chief Compliance Officer) oraz działu prawnego:

- wszelkie zgłoszone, przewidywane lub potencjalne naruszenia danych (np. e-mail wysłany do nieprawidłowych odbiorców, dane osobowe ujawnione nieupoważnionym osobom, naruszenie bezpieczeństwa, zwykle skutkują naruszeniem danych)
- skargi, roszczenia i oskarżenia związane z ochroną danych, składane przez podmioty danych (np. pracowników, klientów, dostawców)
- wnioski związane z ochroną danych, składane przez wszelkie podmioty danych (np. klient pytający o czynności związane z przetwarzaniem jego danych osobowych)
- naruszenia lub potencjalne naruszenia przepisów o ochronie danych, jak również naruszenie niniejszej Polityki ochrony danych
- kary nakładane przez organy ds. ochrony danych
- audyty zalecane przez organy ds. ochrony danych

- wszelkie naruszenia bezpieczeństwa lub incydenty związane z systemami informatycznymi (np. naruszone systemy, awarie systemu, próby włamania, wtargnięcia do systemów, próby uzyskania nieupoważnionego dostępu), które mogą skutkować naruszeniem danych.

Utrata lub kradzież urządzeń mobilnych (laptopów, telefonów komórkowych, tabletów, urządzeń USB) może skutkować potencjalnym naruszeniem danych, dlatego tego rodzaju incydenty należy również zgłaszać lokalnemu DPC/DPO, Dyrektorowi ds. Zgodności (Chief Compliance Officer) oraz Dyrektorowi ds. IT. Ponadto lokalna kadra kierownicza musi:

- prowadzić dokumentację wszystkich incydentów i zdarzeń wymienionych powyżej
- przechowywać wszystkie właściwe dokumenty, komunikaty i środki podjęte w związku z tymi incydentami oraz wnioski w osobnej teczce, która będzie dostępna na żądanie

Wszystkich wyznaczonych DPO i DPC, jak również wszelkie dalsze zmiany należy zgłaszać, wraz ze wszystkimi danymi kontaktowymi do Dyrektorowi ds. Zgodności (Chief Compliance Officer) i/lub działu prawnego Grupy.

5. Zakres odpowiedzialności i obowiązki, audyt

Personel Grupy i lokalna kadra kierownicza odpowiada za zapewnienie, że wszystkie istotne środki organizacyjne, kadrowe i techniczne są wdrożone, dzięki czemu wszelkiego rodzaju przetwarzanie danych osobowych jest przeprowadzane zgodnie z krajowym ustawodawstwem dotyczącym ochrony danych. Stosowanie się do tych wymogów jest obowiązkiem wszystkich pracowników.

Wszyscy pracownicy DYWIDAG (włącznie z pracownikami tymczasowymi i wynajmowanymi), kadra kierownicza i usługodawcy, którzy przetwarzają dane osobowe na terenie DYWIDAG, korzystają z systemów i sprzętu do przetwarzania danych DYWIDAG lub są z nimi połączeni, są zobowiązani do przestrzegania niniejszej polityki.

Dział audytu wewnętrznego Grupy będzie okresowo sprawdzać zgodność z niniejszą Polityką Ochrony Danych poprzez przeprowadzane na miejscu lub zdalnie weryfikacje ochrony danych i/lub bezpieczeństwa informatycznego, lub podobne weryfikacje. Wykonując to zadanie, dział audytu wewnętrznego będzie upoważniony do wynajęcia zewnętrznych audytorów lub ekspertów w tej dziedzinie.