

POLITYKA OCHRONY DANYCH OSOBOWYCH

Nazwa Administratora:

Performance Media P.S.A

ul. Idzikowskiego 19

02-704 Warszawa

KRS 0000956624, NIP 521-374-29-52

SPIS TREŚCI

I.	WPROWADZENIE.....	3
	PODSTAWA PRAWNA	3
	SŁOWNICZEK	3
II.	OGÓLNA INSTRUKCJA DLA ADMINISTRATORA / IOD / ASI	6
	OBOWIĄZKI ADMINISTRATORA	6
	OBOWIĄZKI INSPEKTORA OCHRONY DANYCH	7
	REJESTROWANIE CZYNNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH	8
	ANALIZA RYZYKA.....	8
	ŚRODKI OCHRONY DANYCH	9
	UPOWAŻNIENIE (POLECENIE) DO PRZETWARZANIA DANYCH OSOBOWYCH.....	9
III.	OGÓLNA INSTRUKCJA DLA ADMINISTRATORA SYSTEMU INFORMATYCZNEGO	10
	OBOWIĄZKI ADMINISTRATORA SYSTEMU INFORMATYCZNEGO	10
	PROCEDURA EWIDENCJONOWANIA.....	11
IV.	OGÓLNA INSTRUKCJA DLA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH ORAZ DLA ADMINISTRATORA / IOD / ASI	12
	OBOWIĄZKI OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH	12
	CZYM SĄ DANE OSOBOWE?	13
	KIEDY MOŻNA PRZETWARZAĆ DANE OSOBOWE ZWYKŁE?	13
	KIEDY MOŻNA PRZETWARZAĆ DANE OSOBOWE SZCZEGÓLNYCH KATEGORII?	14
	ZASADY PRZETWARZANIA DANYCH OSOBOWYCH	14
	MONITORING WIZYJNY.....	15
	MONITORING POCZTY ELEKTRONICZNEJ.....	15
V.	POSTANOWIENIA SZCZEGÓŁOWE DOTYCZĄCE PODMIOTU	15
VI.	POSTANOWIENIA KOŃCOWE.....	17

Performance Media P.S.A.

ul. Idzikowskiego 19

02-704 Warszawa

I. WPROWADZENIE

Polityka Ochrony Danych Osobowych, zwana dalej Polityką Ochrony Danych, została sporządzona w związku z wymaganiami Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych – dalej Rozporządzenie UE) oraz ustawy o ochronie danych osobowych.

Niniejszy dokument wraz z załącznikami stanowi zbiór spójnych, precyzyjnych reguł i procedur, według których Podmiot buduje, zarządza oraz udostępnia zasoby i systemy informacyjne i informatyczne. Ustanawia przewidziane do wykonania działania oraz sposób ustanowienia zasad i reguł postępowania, koniecznych do zapewnienia właściwej ochrony przetwarzanych danych osobowych. Polityka Ochrony Danych ustanawia zasady bezpieczeństwa przetwarzania danych osobowych, które powinny być przestrzegane i stosowane w Podmiocie przez wszystkie osoby przetwarzające dane osobowe. Polityka Ochrony Danych reguluje zasady organizacji pracy przy zbiorach danych osobowych przetwarzanych w systemie informatycznym oraz metodami tradycyjnymi. Opisano w niej również zagrożenia bezpieczeństwa przetwarzanych danych osobowych oraz sposoby reakcji na przypadki naruszeń bezpieczeństwa.

Niniejszy dokument wraz z załącznikami pełni również funkcję informacyjną i edukacyjną, poprzez zaprezentowanie obowiązków i odpowiedzialności osób związanych z przetwarzaniem danych osobowych.

Podmiot stosuje adekwatne do sytuacji środki, aby zapewnić bezpieczeństwo przetwarzanych danych osobowych.

PODSTAWA PRAWNA

Zasady przetwarzania danych osobowych regulują przepisy powszechnie obowiązującego prawa, a w szczególności:

- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.
- Ustawa o ochronie danych osobowych z dnia 10 maja 2018 r.

SŁOWNICZEK

Administrator – Administrator danych osobowych, będący organem, jednostką organizacyjną, podmiotem lub osobą fizyczną, decydujący o celach i środkach przetwarzania danych osobowych. W przypadku użycia pojęcia „ADO” należy rozumieć je jako osoby uprawnione do reprezentacji. **Performance Media P.S.A. z siedzibą w Warszawie (02-704 Warszawa), ul. Idzikowskiego 19, reprezentowana przez** Adama Oskaldowicza - Prezesa Zarządu albo Janusza Zadwornego – Wiceprezesa Zarządu (każdy z nich z osobną upoważniony do reprezentacji jednoosobowej) albo Iwonę Kuchtę lub Piotra Panasiuka lub Dariusza Kuchtę jako członków zarządu (upoważnieni do reprezentacji łącznej dwuosobowej).

Performance Media P.S.A.

ul. Idzikowskiego 19

02-704 Warszawa

ASI – Administrator Systemu Informatycznego, będący wyznaczoną przez Administratora osobą odpowiedzialną za prawidłowe funkcjonowanie sprzętu, oprogramowania i ich konserwację, w zakresie wskazanym przez Administratora.

Dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej; możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

Szczególne kategorie danych osobowych – dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, dane biometryczne przetwarzane w celu jednoznacznego zidentyfikowania osoby fizycznej, dane dotyczące zdrowia, seksualności lub orientacji seksualnej oraz dane dotyczące wyroków skazujących oraz czynów zabronionych lub powiązanych środków bezpieczeństwa.

Hasło – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.

Identyfikator użytkownika – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.

Integralność danych – właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany.

IOD – Inspektor Ochrony Danych, będący wyznaczoną przez Administratora osobą nadzorującą stosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, odpowiednich do zagrożeń oraz kategorii danych objętych ochroną.

Incydent bezpieczeństwa informacji – Incydem bezpieczeństwa informacji jest zdarzenie, którego bezpośrednim lub pośrednim skutkiem jest lub może być naruszenie bezpieczeństwa aktywów informacyjnych.

Naruszenie ochrony danych osobowych – oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Odbiorca – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania.

Strona trzecia – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe.

Osoba upoważniona – osoba posiadająca formalne upoważnienie-polecenie wydane przez Administratora lub przez osobę wyznaczoną, uprawniona do przetwarzania danych osobowych.

Podmiot – podmiot dla którego niniejsza Polityka Ochrony Danych zostaje opracowana i wdrożona.
Performance Media P.S.A. z siedziba w Warszawie (02-704 Warszawa), ul. Idzikowskiego 19

Performance Media P.S.A.

ul. Idzikowskiego 19
02-704 Warszawa

Podmiot przetwarzający – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora.

Polityka Ochrony Danych – niniejszy dokument Polityki Ochrony Danych Osobowych.

Poufność danych – właściwość zapewniająca, że dane osobowe nie są udostępniane nieupoważnionym do ich przetwarzania osobom lub podmiotom.

Przetwarzanie danych – oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

Pseudonimizacja – oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;

PUODO – Prezes Urzędu Ochrony Danych Osobowych, będący organem powołanym do spraw z zakresu ochrony danych osobowych.

Rozliczalność – właściwość zapewniająca, że działania osoby na danych osobowych mogą być przypisane w sposób jednoznaczny tylko tej osobie, nadto właściwość zapewniająca możliwość udowodnienia realizacji praw osób, których dane osobowe są przetwarzane.

Rozporządzenie UE – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.

Ryzyko – kombinacja prawdopodobieństwa zdarzenia i jego konsekwencji (skutków).

System informatyczny – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

Upoważnienie – dowód, iż każda osoba działająca z upoważnienia Administratora lub podmiotu przetwarzającego i mająca dostęp do danych osobowych, przetwarza je wyłącznie na polecenie Administratora.

Usuwanie danych – zniszczenie danych osobowych lub ich modyfikacja, która uniemożliwia ustalenie tożsamości osoby, której dane dotyczą.

Uwierzytelnianie – działanie, którego celem jest weryfikacja deklarowanej tożsamości osoby lub podmiotu.

Użytkownik – osoba, która posiada konto w systemie informatycznym należącym do Podmiotu.

Zabezpieczenie danych w systemie informatycznym – wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.

Zbiór danych – uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.

Zgoda osoby, której dane dotyczą – oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.

Performance Media P.S.A.

ul. Idzikowskiego 19
02-704 Warszawa

II. OGÓLNA INSTRUKCJA DLA ADMINISTRATORA / IOD / ASI

OBOWIĄZKI ADMINISTRATORA

1. zapewnienie podstaw prawnych do przetwarzania danych osobowych od chwili zebrania danych osobowych do chwili ich usunięcia, w szczególności poprzez stosowanie obowiązków informacyjnych, zgodnie z wykazem treści obowiązków informacyjnych, stosowanych w Podmiocie.
2. zapewnienie rozliczalności, tj. kontroli nad tym, jakie dane osobowe, przez kogo i kiedy zostały wprowadzone, edytowane lub usunięte,
3. dbałość o prawidłowe przetwarzanie danych osobowych, w szczególności poprzez zapewnienie aktualności, adekwatności oraz merytorycznej poprawności danych osobowych przetwarzanych w określonym przez nich celu,
4. dbałość o prawidłową realizację zasady czasowości, w szczególności poprzez zapewnienie usuwania danych osobowych po czasie niezbędnego ich przetwarzania,
5. wdrożenie środków organizacyjnych (procedur) i technicznych ochrony danych osobowych,
6. analiza ryzyka wdrażanych i wdrożonych procedur, środków bezpieczeństwa, zasobów i procesów przetwarzania danych osobowych przy użyciu,
7. egzekwowanie rozwoju środków bezpieczeństwa przetwarzania danych osobowych,
8. prowadzenie dokumentacji opisującej zastosowaną politykę bezpieczeństwa przetwarzania danych osobowych (niniejsza Polityka Ochrony Danych oraz wynikające z niej instrukcje i procedury),
9. prowadzenie rejestru czynności przetwarzania danych osobowych,
10. prowadzenie rejestru kategorii czynności przetwarzania danych osobowych,
11. nadawanie i uchylanie upoważnień do przetwarzania danych osobowych przez pracowników i inne osoby, na podstawie przyjętych wzorów upoważnień dla pracowników oraz upoważnień dla umów cywilnoprawnych,
12. prowadzenie rejestru osób upoważnionych do przetwarzania danych osobowych i przechowywanie wydanych upoważnień do przetwarzania danych osobowych,
13. wdrożenie środków zapoznania z przepisami dotyczącymi ochrony danych osobowych i zasadami w tym przedmiocie oraz zagrożeniami związanymi z przetwarzaniem danych przez pracowników Podmiotu,
14. zapewnienie zapoznania osób upoważnionych do przetwarzania danych osobowych z wewnętrznymi procedurami przetwarzania danych osobowych,
15. powierzanie czynności przetwarzania danych osobowych podmiotom, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, na podstawie umów powierzenia danych osobowych lub innych instrumentów prawnych, spełniających wymogi powierzenia przetwarzania danych osobowych,
16. zapewnienie, że powierzenie przetwarzania danych osobowych podmiotom przetwarzającym, odbywa się zgodnie z Procedurą powierzenia przetwarzania danych osobowych,

Performance Media P.S.A.

ul. Idzikowskiego 19

02-704 Warszawa

17. wyznaczenie Inspektora Ochrony Danych, gdy obowiązek jego wyznaczenia wynika z obowiązujących przepisów,
18. zapewnienie środków i organizacyjnej odrębności Inspektorowi Ochrony Danych, niezbędnych do niezależnego wykonywania przez niego zadań,
19. udokumentowanie powołania Inspektora Ochrony Danych poprzez wydanie oświadczenia o powołaniu IOD,
20. zawiadomienie Prezesa Urzędu Ochrony Danych Osobowych o wyznaczeniu Inspektora Ochrony Danych,
21. wyznaczenie Administratora Systemu Informatycznego,
22. udokumentowanie powołania Administratora Systemu Informatycznego poprzez wydanie oświadczenia o powołaniu ASI,
23. w przypadku stwierdzenia naruszenia ochrony danych osobowych, prowadzenie działań zgodnych z procedurą postępowania z naruszeniami ochrony danych osobowych,
24. w przypadku udostępniania danych osobowych, stosowanie procedury udostępniania danych osobowych.

OBOWIĄZKI INSPEKTORA OCHRONY DANYCH, GDY POWOŁANY

1. informowanie Podmiotu oraz jego pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy Rozporządzenia UE oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie, w tym w szczególności wsparcie merytoryczne Podmiotu w jego obowiązkach:
 - prowadzenia rejestru czynności przetwarzania danych osobowych, rejestru kategorii czynności przetwarzania danych osobowych – jednakże nie końcowe zatwierdzanie ich kolejnych wersji,
 - realizacji praw osób, których dotyczą przetwarzane dane osobowe zgodnie z przyjętą procedurą realizacji żądań podmiotów danych oraz ich odnotowywanie w rejestrze realizacji żądań podmiotów danych,
 - zgodnego z prawem powierzania przetwarzania danych osobowych, w szczególności poprzez weryfikację lub formułowanie umów powierzenia przetwarzania danych osobowych lub innych instrumentów prawnych, służących w tym celu,
 - realizacji obowiązków, w przypadku wystąpienia naruszeń ochrony danych osobowych,
2. monitorowanie przestrzegania Rozporządzenia UE, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk Podmiotu w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty,
3. udzielanie na żądanie zaleceń co do ocen skutków dla ochrony danych osobowych oraz monitorowanie ich wykonania,
4. współpraca z organem nadzorczym,

Performance Media P.S.A.

ul. Idzikowskiego 19
02-704 Warszawa

5. pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 Rozporządzenia UE, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

W przypadku braku powołania Inspektora Ochrony Danych działania realizuje Podmiot.

REJESTROWANIE CZYNNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH

Administrator, przy wsparciu merytorycznym IOD, prowadzi rejestr czynności przetwarzania danych osobowych, w którym zamieszcza wszystkie następujące informacje:

1. imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów, a także gdy ma to zastosowanie – przedstawiciela administratora oraz inspektora ochrony danych,
2. cele przetwarzania,
3. opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych,
4. kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych,
5. gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazania, o których mowa w art. 49 ust. 1 akapit drugi Rozporządzenia UE, dokumentacja odpowiednich zabezpieczeń,
6. jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych,
7. jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 Rozporządzenia UE.

ANALIZA RYZYKA

W ramach obowiązków monitorowania przestrzegania Rozporządzenia UE, innych przepisów Unii lub przepisów krajowych oraz polityk Podmiotu w dziedzinie ochrony danych osobowych, uwzględnia się ryzyko związane z realizowanymi operacjami przetwarzania, w szczególności przez jego szacowanie i formułowanie zaleceń.

Poszczególne:

1. zasoby Podmiotu (takie jak budynek, pomieszczenia, serwer, serwerownia, oprogramowanie, archiwum, personel),
2. czynności przetwarzania danych osobowych – uzupełniająco, w stosunku do uprzednio przeprowadzonej analizy ryzyka w odniesieniu do zasobów,

należy poddać analizie ryzyka naruszenia praw lub wolności osób, których dotyczą przetwarzane dane.

Analizę ryzyka należy przeprowadzać uwzględniając:

1. charakter przetwarzania danych osobowych,
2. zakres przetwarzania danych osobowych,

Performance Media P.S.A.

ul. Idzikowskiego 19
02-704 Warszawa

3. kontekst przetwarzania danych osobowych,
4. cele przetwarzania danych osobowych,
5. ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia.

Na podstawie tak przeprowadzonej analizy ryzyka, formułuje się zalecenia, w szczególności obejmujące wdrażanie odpowiednich środków technicznych i organizacyjnych ochrony danych osobowych, zmierzających do ograniczenia zdiagnozowanych ryzyk.

Prawo zatwierdzenia zaleceń i podjęcia decyzji o ich wdrożeniu należy do Administratora.

Wdrożenie zaleceń, a także ich wpływ na zdiagnozowane ryzyka należy monitorować, poddawać przeglądowi i w przypadku takiej potrzeby, uaktualniać.

ŚRODKI OCHRONY DANYCH

Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze, Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z Rozporządzeniem UE i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądowi i uaktualniane.

Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze, Administrator i Podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, w tym między innymi w stosownym przypadku:

- pseudonimizację i szyfrowanie danych osobowych,
- zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,
- zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego,
- regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

W zakresie organizacyjnych środków bezpieczeństwa, wykazanych w rejestrze czynności przetwarzania danych osobowych, wchodzi wszelkie środki organizacyjne, przyjęte w celu zwiększenia bezpieczeństwa systemu przetwarzania danych osobowych.

W zakresie technicznych środków bezpieczeństwa wykazanych w rejestrze czynności przetwarzania danych osobowych, należy wymienić wszelkie środki techniczne, wdrożone w celu zapewnienia bezpieczeństwa systemu przetwarzania danych osobowych.

UPOWAŻNIENIE (POLECENIE) DO PRZETWARZANIA DANYCH OSOBOWYCH

1. W Podmiocie do przetwarzania danych osobowych uprawnione są wyłącznie osoby upoważnione do przetwarzania danych osobowych.

Performance Media P.S.A.

ul. Idzikowskiego 19

02-704 Warszawa

2. Administrator jest uprawniony do przyznawania upoważnień (poleceń) w przedmiocie przetwarzania danych osobowych, w drodze pisemnego upoważnienia do przetwarzania danych osobowych.
3. Upoważnienie do przetwarzania danych osobowych następuje wyłącznie na podstawie indywidualnego upoważnienia.
4. Nadanie upoważnienia do przetwarzania danych osobowych musi nastąpić przed rozpoczęciem przetwarzania danych osobowych przez osobę upoważnioną.
5. Administrator lub osoba przez niego upoważniona prowadzi rejestr osób upoważnionych do przetwarzania danych osobowych oraz przechowuje wydane upoważnienia.
6. W przypadku konieczności nadania bądź zmiany upoważnień (np. z powodu zatrudnienia osoby lub zmiany stanowiska pracy), Administrator lub osoba przez niego upoważniona zobowiązany jest do sprawdzenia, czy dana osoba:
 - a. odbyła szkolenie z zakresu przestrzegania zasad przetwarzania danych osobowych,
 - b. zapoznała się z dokumentacją przetwarzania danych osobowych w Podmiocie.
7. Nadanie upoważnienia do przetwarzania danych osobowych wymaga zaznajomienia się z dokumentacją przetwarzania danych osobowych w Podmiocie, w zakresie niezbędnym do czynności wykonywanych w ramach udzielonego upoważnienia.
8. Administrator jest odpowiedzialny za organizację i przeprowadzenie szkoleń z zasad przetwarzania danych osobowych lub zaznajomienie w innej formie osób upoważnionych z zasadami ochrony danych osobowych, w zakresie niezbędnym do czynności wykonywanych w ramach udzielonego upoważnienia.

III. OGÓLNA INSTRUKCJA DLA ADMINISTRATORA SYSTEMU INFORMATYCZNEGO

OBOWIĄZKI ADMINISTRATORA SYSTEMU INFORMATYCZNEGO

1. wdrożenie i utrzymanie środków szyfrowania danych osobowych, przetwarzanych w ramach systemu informatycznego Podmiotu, w szczególności zabezpieczenie środkami ochrony kryptograficznej urządzeń przenośnych służących do przetwarzania danych osobowych (np. laptopy, smartfony),
2. właściwa konfiguracja systemu informatycznego służącego do przetwarzania danych osobowych w Podmiocie, w celu zapewnienia jego zdolności do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,
3. dbałość o utrzymanie i zabezpieczenie serwerów systemu informatycznego służącego do przetwarzania danych osobowych w Podmiocie, niezależnie od tego czy serwer znajduje się w zasobach lokalowych Podmiotu, czy poza nim, a w szczególności zapewnienie jego poufności, integralności, dostępności i odporności,
4. zapewnianie zdolności systemu informatycznego służącego do przetwarzania danych osobowych w Podmiocie, do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego,

Performance Media P.S.A.

ul. Idzikowskiego 19
02-704 Warszawa

5. regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych systemu informatycznego służącego do przetwarzania danych osobowych w Podmiocie, mających zapewnić bezpieczeństwo przetwarzania danych osobowych z jego użyciem,
6. instalacja, konfiguracja, usuwanie, zamawianie licencji i ich przedłużanie, w odniesieniu do oprogramowania używanego w urządzeniach teleinformatycznych stosowanych w systemie teleinformatycznym Podmiotu,
7. nadzór nad pracami podmiotów zewnętrznych, przeprowadzających prace przy naprawach, konserwacjach systemów informatycznych służących do przetwarzania danych osobowych w Podmiocie, w celu zapewnienia zgodności tych czynności z zasadami przyjętymi w Podmiocie,
8. nadawanie, zmiana i wycofywanie identyfikatorów i haseł oraz uprawnień do korzystania z aplikacji i programów osobom upoważnionym do przetwarzania danych osobowych w Podmiocie,
9. nadzór nad prawidłowym wdrożeniem i funkcjonowaniem systemu sporządzania kopii bezpieczeństwa wszelkich nośników informacji, służących do przetwarzania danych osobowych w Podmiocie,
10. podejmowanie działań w przypadku podejrzenia lub wykrycia naruszeń bezpieczeństwa w systemie zabezpieczeń systemu informatycznego służącego do przetwarzania danych osobowych w Podmiocie, zgodnie z procedurą postępowania z naruszeniami ochrony danych osobowych,
11. podejmowanie działań w przypadku podejrzenia lub wykrycia incydentów bezpieczeństwa informacji w systemie zabezpieczeń systemu informatycznego służącego do przetwarzania danych osobowych w Podmiocie,
12. świadczenie pomocy technicznej w zakresie obsługi oprogramowania i urządzeń używanych w ramach systemu informatycznego służącego do przetwarzania danych osobowych w Podmiocie,
13. zabezpieczenie urządzeń służących do przetwarzania danych osobowych w Podmiocie,
14. zabezpieczenie haseł ASI i zapewnienie dostępu do nich w sytuacjach wyższej konieczności / natury siły wyższej / niezdolności ASI do użycia haseł,
15. nadzór nad przestrzeganiem procedury kontroli dostępu do systemu informatycznego,
16. nadzór nad przestrzeganiem procedury zabezpieczenia antywirusowego,
17. nadzór nad przestrzeganiem procedury ewidencjonowania urządzeń i nośników informacji,
18. nadzór nad przestrzeganiem procedury usuwania urządzeń i nośników informacji,
19. nadzór nad przestrzeganiem procedury przeglądów i konserwacji systemu informatycznego,
20. nadzór nad przestrzeganiem procedury postępowania za hasłami i plikami dostępowymi,
21. nadzór nad przestrzeganiem procedury zabezpieczenia antywirusowego,
22. pozostałe działania przewidziane Polityką Ochrony Danych.

PROCEDURA EWIDENCJONOWANIA

ASI jest zobowiązany do ewidencjonowania wszelkich czynności wykonywanych w systemie informatycznym służącym do przetwarzania danych osobowych w Podmiocie, a także do ewidencjonowania urządzeń i nośników, służących do przetwarzania danych osobowych. Ewidencjonowanie następuje w:

1. rejestrze napraw, przeglądów i konserwacji systemu informatycznego,

Performance Media P.S.A.

ul. Idzikowskiego 19
02-704 Warszawa

2. rejestrze czynności w systemie informatycznym,
3. rejestrze urządzeń i nośników, służących do przetwarzania danych osobowych.

IV. OGÓLNA INSTRUKCJA DLA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH ORAZ DLA ADMINISTRATORA / IOD / ASI

OBOWIĄZKI OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

Ustanawia się poniższe obowiązki dotyczące przetwarzania danych osobowych.

Każda osoba jest uprawniona do przetwarzania danych osobowych tylko po otrzymaniu upoważnienia do tej czynności.

Do obowiązków osób upoważnionych do przetwarzania danych osobowych, należy postępowanie zgodnie z ustalonymi regulacjami wewnętrznymi dotyczącymi przetwarzania danych osobowych, a w szczególności:

1. zachowanie w tajemnicy danych osobowych oraz informacji o sposobach ich zabezpieczenia, również po ustaniu zatrudnienia lub innego stosunku cywilnoprawnego,
2. niewykorzystywanie w celach pozasłużbowych danych osobowych, urządzeń i programów służących do przetwarzania danych osobowych w Podmiocie,
3. zabezpieczanie obszaru, w którym przetwarza się dane osobowe przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych, przy użyciu środków zapewnionych przez Podmiot,
4. zapewnianie, aby przebywanie osób nieupoważnionych do przetwarzania danych osobowych w obszarze ich przetwarzania, następowało wyłącznie w obecności osoby upoważnionej do przetwarzania danych osobowych i pod jej nadzorem,
5. informowanie IOD lub Administratora o wszelkich podejrzeniach naruszenia lub zauważonych naruszeniach oraz słabościach systemu przetwarzającego dane osobowe, zgodnie z procedurą postępowania z naruszeniami ochrony danych osobowych,
6. niezwłoczne przekazywanie IOD lub Administratorowi wszelkich zgłoszeń dotyczących przetwarzania danych osobowych przez Podmiot, zgodnie z procedurą realizacji żądań podmiotu danych,
7. realizacja obowiązku informacyjnego w stosunku do osób, których dane osobowe są przetwarzane przez Podmiot w przypadku, gdy to osoba upoważniona jest osobą zbierającą te dane, zgodnie z procedurą realizacji obowiązku informacyjnego,
8. używanie wyłącznie programów i aplikacji dopuszczonych do używania przez ASI lub Administratora,
9. ochrona danych osobowych oraz środków przetwarzających dane osobowe przed nieuprawnionym dostępem, ujawnieniem, modyfikacją, zniszczeniem lub zniekształceniem,
10. znajomość i stosowanie Polityki Ochrony Danych w niniejszej części nr IV oraz procedur przetwarzania danych osobowych, do przestrzegania których osoba została zobowiązana przez Podmiot.

Performance Media P.S.A.

ul. Idzikowskiego 19
02-704 Warszawa

Postępowanie sprzeczne z powyższymi zobowiązaniami, może być uznane przez Administratora za ciężkie naruszenie obowiązków pracowniczych w rozumieniu art. 52 § 1 pkt 1 Kodeksu Pracy lub za naruszenie umowy cywilnoprawnej obowiązującej pomiędzy stronami tej umowy.

CZYM SĄ DANE OSOBOWE?

Za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

Danymi osobowymi będą zarówno takie dane, które pozwalają na określenie tożsamości konkretnej osoby, jak i takie, które nie pozwalają na jej natychmiastową identyfikację, ale są, przy pewnym nakładzie kosztów, czasu i działań, wystarczające do jej ustalenia.

Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne.

Rozróżniamy trzy rodzaje danych osobowych:

1. zwykłe,
2. szczególne („wrażliwe”): głównie dotyczące zdrowia, ale także ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane dotyczące seksualności lub orientacji seksualnej oraz dane genetyczne i biometryczne przetwarzane w celu jednoznacznego zidentyfikowania osoby fizycznej,
3. dotyczące wyroków skazujących i naruszeń prawa.

KIEDY MOŻNA PRZETWARZAĆ DANE OSOBOWE ZWYKŁE?

Przetwarzanie zwykłych danych osobowych jest dopuszczalne tylko wtedy, gdy:

1. osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów,
2. przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy,
3. przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na Administratorze,
4. przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej,
5. przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi (dotyczy tylko podmiotów publicznych),
6. przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych w szczególności, gdy osoba której dane dotyczą, jest dzieckiem (nie dotyczy podmiotów publicznych).

Performance Media P.S.A.

ul. Idzikowskiego 19
02-704 Warszawa

KIEDY MOŻNA PRZETWARZAĆ DANE OSOBOWE SZCZEGÓLNYCH KATEGORII?

Nie wolno przetwarzać danych osobowych szczególnych kategorii, z wyjątkiem sytuacji, gdy (najczęściej):

1. osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach, chyba że prawo Unii lub prawo państwa członkowskiego przewidują, iż osoba, której dane dotyczą, nie może uchylić zakazu,
2. przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez Administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej,
3. przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa Unii Europejskiej lub prawa państwa członkowskiego,
4. przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń.

ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

Ustanawia się poniższe zasady przetwarzania danych osobowych w Podmiocie.

Podmiot i osoby upoważnione do przetwarzania danych osobowych realizują obowiązki poprzez dołożenie szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, zapewniając aby dane te były:

1. **Przetwarzane zgodnie z prawem.**
Przetwarzanie należy realizować zgodnie z wszelkimi normami prawa, zarówno tymi już istniejącymi w momencie wejścia w życie Rozporządzenia UE, jak i tymi, które dopiero później zostały wprowadzone do porządku prawnego.
2. **Zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami.**
3. **Merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane.**
Informacje wynikające z danych przetwarzanych przez Administratora muszą być zgodne z prawdą, kompletne oraz odpowiadające aktualnemu stanowi faktycznemu. Administrator przetwarza dane tylko w takim zakresie, w jakim jest to niezbędne do wypełnienia celu, w jakim dane są przez niego przetwarzane.
4. **Przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.**
5. **Administrator stosuje środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, odpowiednią do zagrożeń oraz kategorii danych objętych ochroną.**

W szczególności, należy zabezpieczać dane przed ich udostępnieniem osobom nieupoważnionym, zabranianiem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów powszechnie obowiązującego prawa oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

Performance Media P.S.A.

ul. Idzikowskiego 19
02-704 Warszawa

Dodatkowo Podmiot zapewnia bezpieczeństwo przetwarzanych danych osobowych, w szczególności poprzez:

1. **Poufność danych osobowych.**

Dane osobowe nie mogą być ujawniane osobom nieupoważnionym lub nieuprawnionym.

2. **Integralność danych osobowych.**

Dane osobowe muszą być kompletne i niezmieniane w sposób nieuprawniony.

3. **Rozliczalność działań na danych osobowych.**

Wszystkie istotne czynności wykonane przy przetwarzaniu danych osobowych, takie jak ich wprowadzanie lub edycja, muszą podlegać zarejestrowaniu tak, aby było możliwe zidentyfikowanie osoby, która daną czynność wykonała.

Osoby upoważnione do przetwarzania danych osobowych, przy wykonywaniu czynności służbowych, zobowiązane są przestrzegać wyżej wymienionych zasad.

MONITORING WIZYJNY

(regulacje w pełnej wersji Polityki).

MONITORING POCZTY ELEKTRONICZNEJ

(regulacje w pełnej wersji Polityki)

V. POSTANOWIENIA SZCZEGÓŁOWE DOTYCZĄCE PODMIOTU

ADMINISTRATOR DANYCH OSOBOWYCH I IOD

Administratorem danych osobowych jest **Performance Media P.S.A. z siedzibą w Warszawie (02-704 Warszawa), ul. Idzikowskiego 19**

Administrator nie powołał Inspektora Danych Osobowych. We wszystkich kwestiach dotyczących przetwarzania danych osobowych oraz praw przysługujących podmiotom danych należy się kontaktować z Administratorem pod następujący adres e-mail: rodo@performance-media.pl.

CELE, PODSTAWA PRAWNA I CZAS PRZETWARZANIA DANYCH OSOBOWYCH

Dane osobowe przetwarzane są w następujących celach:

1. realizacji zawartej umowy – przez okres obowiązywania umowy (podstawa prawna: art. 6 ust. 1 lit. b RODO);
2. dochodzenia, obrony i ustalania ewentualnych roszczeń z tytułu zawartej umowy – przez okres wynikający z okresu przedawnienia (podstawa prawna: art. 6 ust. 1 lit. f RODO);
3. realizacji obowiązków rachunkowych i podatkowych – przez okres 5 lat od końca roku kalendarzowego (podstawa prawna: art. 6 ust. 1 lit. c RODO);

Performance Media P.S.A.

ul. Idzikowskiego 19
02-704 Warszawa

4. marketingu, promocji i sprzedaży usług (podstawa prawna : art. 6 ust. 1 lit. a RODO) – o ile taka zgoda zostanie wyrażona przy zawarciu umowy – przez okres 5 lat lub do momentu cofnięcia zgody.

W celu realizacji zawartej umowy o przeprowadzenie szkolenia, dane osobowe są przetwarzane w zakresie koniecznym do realizacji zawartej umowy. Wszystkie inne dane osobowe są przetwarzane, gdy jest to niezbędne do zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa lub innych obowiązujących regulacji.

Wszystkie inne dane osobowe są przetwarzane w szczególnych przypadkach po wyrażeniu odrębnej zgody na ich przetwarzanie (art. 6 ust. 1 lit. a RODO), którą podmiot danych ma prawo wycofać w dowolnym momencie. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem (art. 7 ust. 3 RODO).

ODBIORCY DANYCH OSOBOWYCH

Dane osobowe mogą być udostępniane podmiotom uprawnionym na podstawie przepisów prawa. Dostęp do danych osobowych mają również upoważnieni pracownicy Administratora, którzy muszą przetwarzać dane osobowe w ramach wykonywanych obowiązków i zadań służbowych.

Odbiorcami danych mogą być także inne podmioty, którym Administrator zleci wykonanie określonych czynności, z którymi wiąże się konieczność przetwarzania danych osobowych, np. podmioty świadczące usługi z zakresu ochrony mienia i osób, usługi pocztowe i kurierskie, usługi przewozowe, księgowość itp. Dane osobowe mogą być także przekazywane stronom umów zawieranych przez Administratora, jeżeli będzie to konieczne do realizacji tych umów i będzie wynikało z zawartej umowy.

Dane osobowe nie będą przetwarzane w sposób zautomatyzowany i nie podlegają profilowaniu.

Jako agencja marketingu internetowego, Podmiot korzysta z usług firm, dzięki którym zapewnia najwyższy standard obsługi. W związku z tym dane osobowe mogą zostać im przekazane do przetwarzania na zlecenie Podmiotu. Dzieje się tak najczęściej w przypadku współpracy z konkretnym usługodawcą lub podwykonawcą, m.in. w związku ze świadczeniem usług pozycjonowania stron, pozycjonowania lokalnego, Google Ads, Facebook Ads. W takiej sytuacji przekazanie danych nie uprawnia innych podmiotów do dowolnego ich przetwarzania, a jedynie do korzystania z nich w celach wyrażnie przez Podmiot wskazanych. W żadnym przypadku przekazanie danych nie zwalnia Administratora z odpowiedzialności za ich przetwarzanie.

W związku z korzystaniem przez Podmiot z mediów społecznościowych, dane osobowe mogą być przekazywane właścicielom portali: m.in. Facebook, LinkedIn, YouTube, Instagram.

Dostawcy Administratora mają siedzibę głównie w Polsce i w innych krajach Europejskiego Obszaru Gospodarczego (EOG).

PRAWA OSÓB, W ZWIĄZKU Z PRZETWARZANIEM DANYCH OSOBOWYCH

Każda osoba, która przekazała Administratorowi dane osobowe, ma prawo do:

1. dostępu do treści swoich danych,
2. sprostowania swoich danych,
3. usunięcia swoich danych, jeżeli:

Performance Media P.S.A.

ul. Idzikowskiego 19
02-704 Warszawa

- wycofa swoją zgodę na przetwarzanie danych osobowych,
 - dane osobowe przestaną być niezbędne do celów, w których zostały zebrane lub w których były przetwarzane,
 - wniesie sprzeciw wobec wykorzystywania swoich danych w celach marketingowych,
 - wniesie sprzeciw wobec wykorzystywania swoich danych w celu dostosowania naszych usług do swoich preferencji,
 - dane osobowe są przetwarzane niezgodnie z prawem,
4. ograniczenia przetwarzania swoich danych,
 5. wniesienia sprzeciwu wobec przetwarzania swoich danych,
 6. przenoszenia swoich danych,
 7. cofnięcia zgody na przetwarzanie w dowolnym momencie, o ile następuje ono na podstawie zgody. Cofnięcie zgody nie wpływa na przetwarzanie danych dokonywane przed jej cofnięciem.

Każdej osobie przysługuje prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna, że przetwarzanie jej danych osobowych narusza przepisy obowiązującego prawa.

Podanie danych osobowych w celach marketingowych (w tym prowadzenia działań w mediach społecznościowych) jest dobrowolne.

VI. POSTANOWIENIA KOŃCOWE

1. Polityka Ochrony Danych jest dokumentem obowiązującym w Podmiocie w zakresie wdrażania, przestrzegania i weryfikacji zasad ochrony danych osobowych.
2. Każda osoba odpowiedzialna za wdrażanie zasad przetwarzania danych osobowych w Podmiocie oraz ich monitorowanie, w szczególności przedstawiciele kierownictwa oraz Inspektor Ochrony Danych, mają obowiązek zapoznania się z niniejszą Polityką Ochrony Danych oraz do jej przestrzegania.
3. Każda osoba upoważniona do przetwarzania danych osobowych w Podmiocie jest zobowiązana do zapoznania się z częścią IV niniejszej Polityki Ochrony Danych oraz do jej przestrzegania.
4. Naruszenie zasad wynikających z Polityki Ochrony Danych może stanowić podstawę wszczęcia stosownego postępowania, w tym dyscyplinarnego, czy również w celu dochodzenia roszczeń przeciwko sprawcy naruszenia.
5. Polityka Ochrony Danych wraz z załącznikami wchodzi w życie z dniem jej podpisania przez Administratora.
6. W przedmiocie spraw nieuregulowanych Polityką Ochrony Danych, zastosowanie znajdują przepisy prawa powszechnie obowiązującego, w szczególności Rozporządzenia UE.

OSTATNIA AKTUALIZACJA: LUTY 2025