

POLITYKA OCHRONY DANYCH OSOBOWYCH

dla

**TOM MEDIA SPÓŁKA Z OGRANICZONĄ
ODPOWIEDZIALNOŚCIĄ**

Ul. Legionów Polskich 129

41-310 Dąbrowa Górnicza

POLITYKA OCHRONY DANYCH OSOBOWYCH w TOM MEDIA SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

SPIS TREŚCI

I. POSTANOWIENIA WSTĘPNE	3
II. DEFINICJE	3
III. ZASADY OCHRONY DANYCH OSOBOWYCH	3
IV. CZĘŚCI SKŁADOWE SYSTEMU OCHRONY DANYCH OSOBOWYCH	4
V. PODSTAWA PRZETWARZANIA DANYCH OSOBOWYCH	5
VI. MINIMALIZACJA DANYCH	5
VII. REJESTR CZYNNOŚCI PRZETWARZANIA DANYCH	6
VIII. INWENTARYZACJA DANYCH	6
VIII. OBSŁUGA PRAW JEDNOSTKI I OBOWIĄZKÓW INFORMACYJNYCH	6
X. ZAPEWNIENIE BEZPIECZEŃSTWA DANYCH	9
XI. PRZETWARZAJĄCY	9
XII. PROCEDURY	10

I. POSTANOWIENIA WSTĘPNE

1. Przedmiotowy dokument stanowi Politykę Ochrony Danych Osobowych (dalej PODO) sporządzoną w oparciu o rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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) (Dz.U.U.E.L.119.1 – dalej jako rozporządzenie RODO).
2. Niniejsze PODO zawiera wytyczne dotyczące ochrony danych osobowych, które obowiązują u administratora danych, przetwarzającego dane w rozumieniu art. 4 RODO.
3. Wdrożenie i utrzymanie PODO spoczywa na administratorze danych,
4. Administrator danych winien powołać Inspektora ochrony danych, albo Pełnomocnika ds. ochrony danych, którzy w imieniu administratora danych, sprawują nadzór i monitoring przestrzegania PODO,
5. Do stosowania przedmiotowego PODO jest zobowiązany administrator danych, jak również komórki organizacyjne przetwarzające dane osobowe oraz personel administratora danych.

II. DEFINICJE

Polityka/PODO – oznacza niniejszą Politykę ochrony danych osobowych.

RODO oznacza rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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) (Dz.U.U.E.L.119.1.).

Dane oznaczają dane osobowe, dane genetyczne, dane biometryczne oraz dane dotyczące zdrowia, o których mowa w art. 4 RODO.

Dane wrażliwe oznaczają dane specjalne wymienione w art. 9 ust. 1 RODO i dane karne wymienione w art. 10 RODO.

Dane dzieci oznaczają dane osób poniżej 16 roku życia.

Osoba oznacza osobę fizyczną, którą można bezpośrednio lub pośrednio zidentyfikować na podstawie identyfikatora w postaci imienia i nazwiska, numeru identyfikacyjnego, danych o lokalizacji, identyfikatora internetowego, albo czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

Podmiot przetwarzający oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora.

Profilowanie oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.

IOD/Inspektor lub PdsODO/Pełnomocnik oznacza Inspektora Ochrony Danych Osobowych, albo Pełnomocnika ds. Ochrony Danych Osobowych.

RCPDO lub Rejestr oznacza Rejestr Czynności Przetwarzania Danych Osobowych.

Administrator/podmiot danych oznacza TOM MEDIA SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

III. ZASADY OCHRONY DANYCH OSOBOWYCH

1. Zasady ogólne:
 - 1.1. Zasada legalności – administrator danych przetwarza dane osobowe zgodnie z prawem, w sposób rzetelny i przejrzysty.
 - 1.2. Zasada bezpieczeństwa – administrator danych przetwarza dane osobowe w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych oraz zapewnia właściwy poziom bezpieczeństwa tych danych poprzez podejmowanie odpowiednich stałych działań w zakresie ich ochrony,
 - 1.3. Zasada poszanowania praw jednostki – administrator danych umożliwia osobom fizycznym, których dane przetwarza, do wykonywania przysługującym im praw, oraz realizuje te prawa.

- 1.4. Zasada rozliczalności – administrator danych dokumentuje realizację ciężących na nim obowiązków w zakresie przetwarzania danych osobowych, wynikające z zasad zgodność z prawem, rzetelność i przejrzystość, ograniczania celu, minimalizacji danych, prawidłowość, ograniczania przechowywania, integralności i poufności danych osobowych, po to, by w każdej chwili mógł wykazać, iż jego działania są zgodne z RODO.
2. Zasady szczegółowe:
 - 2.1. Zasada legalizmu – administrator danych przetwarza dane osobowe zgodnie z prawem i w oparciu o przepisy prawne – art. 5 ust. 1 pkt a RODO,
 - 2.2. Zasada rzetelności – administrator danych przetwarza dane osobowe w sposób rzetelny i uczciwy – art. 5 ust. 1 pkt a RODO,
 - 2.3. Zasada przejrzystości – administrator danych przetwarza dane osobowe w sposób przejrzysty dla osoby, której przetwarzane dane dotyczą – art. 5 ust. 1 pkt a RODO,
w Zasada minimalizacji – administrator danych przetwarza dane osobowe tylko i wyłącznie konkretnych celach – art. 5 ust. 1 pkt c RODO, Zasada adekwatności – administrator danych przetwarza dane osobowe tylko i wyłącznie stopniu wynikającym z konkretnego celu – art. 5 ust. 1 pkt b RODO,
 - 2.4. Zasada prawidłowości – administrator danych przetwarza dane osobowe z najwyższą starannością o prawidłowość przetwarzanych danych – art. 5 ust. 1 pkt d RODO,
 - 2.5. Zasada czasowości – administrator danych przetwarza dane osobowe tylko i wyłącznie przez czas wynikający z konkretnego celu – art. 5 ust. 1 pkt e RODO,

IV. CZĘŚCI SKŁADOWE SYSTEMU OCHRONY DANYCH OSOBOWYCH

- IV.1. Podstawa przetwarzania danych – administrator danych działa w oparciu o przepisy prawne i na ich podstawie. Oznacza to, iż Podmiot danych dokonuje internalizacji i weryfikacji podstaw prawnych przetwarzania danych osobowych, oraz zapewnia ich stosowanie i zapisywanie w rejestrze czynności poprzez utrzymanie systemu zarządzania zgodami na przetwarzanie danych i komunikację na odległość, jak również ewidencjonowanie i uszczegółowianie uzasadnienia każdego przypadku, w którym Podmiot danych przetwarza dane osobowe na podstawie prawnie uzasadnionego interesu.
- IV.2. Minimalizacja danych – administrator danych zarządza kompresją danych osobowych w szczególności zaś adekwatnością danych, dostępem do danych oraz okresem ich przechowywania, jak również dokonuje weryfikacji dalszej przydatności danych.
- IV.3. Rejestr czynności – administrator danych tworzy, prowadzi i utrzymuje Rejestr Czynności Przetwarzania Danych Osobowych (RCPDO). RCPDO jest instrumentem za pomocą którego administrator danych, rozlicza zgodność przetwarzania danych z wymogiem ochrony danych osobowych, wskazanym w RODO.
- IV.4. Inwentaryzacja danych – administrator danych dokonuje internalizacji zasobów danych osobowych znajdujących się u administratora danych, rodzajów tych danych, jak również zależności między poszczególnymi zasobami danych. Celem inwentaryzacji danych jest także identyfikacja sposobów wykorzystania danych w szczególności zaś współadministrowania danymi, czy też przypadków przetwarzania danych wrażliwych, danych niezidentyfikowanych, danych dzieci, jak również profilowania.
- IV.5. Obsługa praw jednostki – administrator danych wykonuje obowiązki informacyjne w stosunku do osób, których dane są przez administratora przetwarzane, jak również zapewnia obsługę praw tychże osób poprzez przekazywanie im przy zbieraniu danych, wymaganych przez RODO informacji. Administrator danych dokumentuje również realizację obowiązków informacyjnych, a także weryfikuje i zapewnia możliwość efektywnego wykonania każdego typu żądania. Zapewnia również odpowiednie środki, aby żądania osób były realizowane w terminach i w sposób wymagany przez RODO oraz właściwie dokumentowane. Nadto stosuje procedury w zakresie zawiadamiania osób, których dane osobowe zostały naruszone.
- IV.6. Upoważnienie do przetwarzania danych – administrator danych posiada i zarządza regułami doboru przetwarzających dane na jego rzecz, jak również wymagań co do warunków przetwarzania (umowa powierzenia), oraz zasad weryfikacji wykonywania umów powierzenia.

IV.7. Zmiana danych – administrator danych zarządza zmianami mającymi wpływ na prywatność, co oznacza, że przed uruchamianiem nowych projektów i inwestycji w podmiocie danych, zostaje dokonana ocena wpływu zmiany na ochronę danych, zapewnienie prywatności, zgodności celów przetwarzania, bezpieczeństwa danych i minimalizacji. Administrator danych zarządza zmianą mającą wpływ na prywatność w taki sposób, aby umożliwić zapewnienie odpowiedniego bezpieczeństwa danych osobowych oraz minimalizacji ich przetwarzania. W tym celu zasady prowadzenia projektów i inwestycji przez Podmiot danych odwołują się do zasad bezpieczeństwa danych osobowych i minimalizacji, wymagając oceny wpływu na prywatność i ochronę danych, uwzględnienia i zaprojektowana bezpieczeństwa i minimalizacji przetwarzania danych od początku projektu lub inwestycji.

IV.8. Bezpieczeństwo – administrator danych zapewnia odpowiedni poziom bezpieczeństwa przetwarzania danych poprzez ocenę ryzyka naruszenia danych osobowych podczas czynności przetwarzania danych, ocenę skutków dla ochrony danych tam, gdzie ryzyko naruszenia praw i wolności osób jest stosunkowo wysokie, dostosowanie środków ochrony danych do wystąpienia potencjalnego ryzyka, posiadanie i stosowanie procedur pozwalających na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Prezesowi Urzędu Ochrony Danych.

V. PODSTAWA PRZETWARZANIA DANYCH OSOBOWYCH

V.1. Administrator danych dokumentuje w Rejestrze podstawę prawną dla każdej z czynności przetwarzania danych osobowych,

V.2. Po wskazaniu ogólnej podstawy prawnej, administrator w razie potrzeby dokonuje jej uszczegółowienia. Tym samym w przypadku, gdy podstawą przetworzenia danych jest zgoda, administrator danych wskazuje jej zakres, w przypadku, gdy podstawa przetworzenia jest dokonywana w oparciu o przepis prawa, wskazuje się na konkretny przepis, etc.

V.3. Personel kierownicy administratora danych jest zobowiązany znać podstawy prawne, na jakich kierowana przez niego komórka, dokonuje konkretnych czynności przetwarzania danych osobowych.

V.4. Administrator danych rejestruje zgody osób fizycznych na przetwarzanie jej konkretnych danych w konkretnym celu, czy też zgody na komunikację na odległość (email, telefon, sms, etc.), jak również rejestruje wszelkie odmowy wyrażenia zgody, cofnięcia zgody, a także inne podobne czynności – sprzeciw, ograniczenie zgody, etc.

VI. MINIMALIZACJA DANYCH

VI.1. Minimalizacja dostępu – administrator danych minimalizuje dostęp do danych osobowych poprzez ograniczenia prawne, takie jak zobowiązania do poufności, zakresy upoważnień, etc., ograniczenia fizyczne w postaci stref dostępu, zamykanie pomieszczeń, zamykanie szaf z dokumentacją, zawierająca dane osobowe, etc. oraz ograniczenia informatyczne w postaci ograniczania uprawnień do systemów przetwarzających dane osobowe i zasobów sieciowych, w których dane osobowe są przechowywane.

VI.2. Minimalizacja zakresu – administrator danych w ramach wdrożenia RODO, dokonał weryfikacji zakresu pozyskiwanych danych, zakresu ich przetwarzania i ilość przetwarzanych danych pod kątem adekwatności danych do celów przetwarzania. W zakresie minimalizacji zakresu danych administrator danych winien dokonać okresowego, co najmniej raz na rok, przeglądu ilości przetwarzanych danych i zakresu ich przetwarzania. Administrator danych w ramach procedury zarządzania zmianą, winien stosować mechanizm weryfikacji zmian, co do ilości i zakresu przetwarzania danych (privacy by design).

VI.3. Minimalizacja czasu – administrator danych stosuje mechanizmy kontroli czasookresu trwania danych osobowych w Spółce poprzez weryfikację dalszej przydatności danych. Dane, których przydatność ulega ograniczeniu na skutek upływu czasu są usuwane z rejestrów/akt administratora danych. Dane takie mogą być jednak archiwizowane oraz znajdować się na kopiach zapasowych systemów i informacji przetwarzanych przez administratora danych. Mechanizm archiwizacji i korzystania z archiwów, jak również tworzenia i wykorzystania kopii zapasowych, winien uwzględniać wymagania kontroli nad czasem przetrzymywania danych, w tym również wymagania dotyczące usuwania danych.

VII. REJESTR CZYNNOŚCI PRZETWARZANIA DANYCH

- VII.1.** RCPDO jest instrumentem służącym do dokumentowania czynności przetwarzania danych osobowych. Za pomocą przedmiotowego rejestru administrator danych ma możliwość udowodnienia przed organem nadzoru, że w zakresie przetwarzania danych osobowych przestrzega przepisy RODO – zgodnie z zasadą rozliczalności art. 5 ust. 2 RODO.
- VII.2.** Administrator danych prowadzi RCPDO, w którym rejestruje, w jaki sposób wykorzystuje dane osób fizycznych. Oznacza to, że przedmiotowy Rejestr umożliwia administratorowi rozliczanie obowiązków związanych z ochroną danych.
- VII.3.** W Rejestrze, dla każdej czynności przetwarzania danych, administrator danych, zgodnie z art. 30 RODO, odnotowuje co najmniej: (a) nazwę czynności, (b) cel przetwarzania, (c) opis kategorii osób, (d) opis kategorii danych, (e) podstawę prawną przetwarzania, wraz z wyszczególnieniem kategorii uzasadnionego interesu Spółki, jeśli podstawą jest uzasadniony interes, (f) sposób zbierania danych, (g) opis kategorii odbiorców danych (w tym przetwarzających), (h) informację o przekazaniu danych do państwa trzeciego oraz (g) ogólny opis technicznych i organizacyjnych środków ochrony danych. RCPDO w zależności od potrzeb administratora może zawierać również kolumny nieobowiązkowe, w których może on rejestrować inne informacje. Pełniejsza treść RCPDO może ułatwić zarządzanie zgodnością ochrony danych i rozliczenie się z niej.

VIII. INWENTARYZACJA DANYCH

- VIII.1.** Dane niezidentyfikowane – za pomocą inwentaryzacji administrator danych identyfikuje przypadki, w których przetwarza lub może przetwarzać dane niezidentyfikowane oraz stosuje mechanizmy ułatwiające realizację praw osób, których dotyczą dane niezidentyfikowane.
- VIII.2.** Dane wrażliwe – dzięki inwentaryzacji danych, administrator danych winien identyfikować przypadki, w których przetwarza lub może przetwarzać dane specjalne i dane karne, by móc stosować mechanizmy zapewnienia zgodności z prawem przetwarzania takich danych. W konsekwencji w przypadku zidentyfikowania przypadków przetwarzania danych wrażliwych, administrator danych powinien postępować zgodnie z przyjętą procedurą.
- VIII.3.** Profilowanie – za pomocą inwentaryzacji administrator danych identyfikuje przypadki, w których dokonuje profilowania przetwarzanych danych oraz stosuje mechanizmy zapewniające zgodność procesu profilowania z podstawą prawną. W konsekwencji w przypadku zidentyfikowania przypadków profilowania i zautomatyzowanego podejmowania decyzji, administrator danych powinien postępować zgodnie z przyjętą procedurą.
- VIII.4.** Współadministrowanie – za pomocą inwentaryzacji administrator danych identyfikuje przypadki współadministrowania danymi osobowymi i postępuje w tym zakresie zgodnie z przyjętą procedurą.

VIII. OBSŁUGA PRAW JEDNOSTKI I OBOWIĄZKÓW INFORMACYJNYCH

IX.1 Prawa jednostki

- IX.1.1. Celem realizacji praw jednostki, administrator danych stosuje mechanizmy, które pozwalają na skonsolidowanie danych konkretnych osób, przetwarzanych przez administratora danych, wprowadzanie do nich zmian i ich usuwanie.
- IX.1.2. Administrator danych dochowuje należytej staranności, żeby sposób komunikacji z osobami, których dane przetwarza, jak również styl przekazywanych im informacji, związanych z przetwarzaniem danych, był dla tych osób jasny, czytelny i zrozumiały.
- IX.1.3. Administrator danych umożliwia osobom korzystanie z ich praw poprzez skierowane do tych osób działania informacyjne o ich prawach, sposobie skorzystania z przysługujących im praw w Spółce, metodach kontaktu z Podmiotem danych w celu realizacji tychże praw, etc.

- IX.1.4. Administrator danych stosuje optymalne sposoby identyfikacji i uwierzytelniania osób, w zakresie realizacji praw jednostki i obowiązków informacyjnych.
- IX.1.5. Administrator danych dochowuje należytej staranności, żeby ciężące na Spółce prawne terminy realizacji obowiązków względem osób były przestrzegane.
- IX.1.6. Administrator danych prowadzi rejestr wszelkich obowiązków informacyjnych, zawiadomień i żądań osób.
- IX.2. Żądania osób**
- IX.2.1. Odmowa – w przypadku zgłoszenia przez osobę żądania dotyczącego jej praw, administrator danych informuje osobę, w ciągu miesiąca od otrzymania żądania, o odmowie rozpatrzenia żądania i o prawach osoby z tym związanych.
- IX.2.2. Nieprzetwarzanie – w przypadku zgłoszenia przez osobę żądania dotyczącego jej praw w zakresie braku zgody na przetwarzanie, administrator danych informuje tą że osobę, że nie przetwarza dotyczących ją danych osobowych.
- IX.2.3. Dostęp do danych – w przypadku zgłoszenia przez osobę żądania dotyczącego jej praw w zakresie dostępu do danych, administrator danych zgodnie z art. 15 RODO informuje osobę, czy przetwarza jej dane osobowe oraz wskazuje szczegóły przetwarzania, (zakres odpowiada obowiązkowi informacyjnemu przy zbieraniu danych). Administrator danych udziela także osobie dostępu do danych jej dotyczących poprzez wydanie tej osobie kopii danych jej dotyczących.
- IX.2.4. Kopia danych – w przypadku zgłoszenia przez osobę żądania dotyczącego wydania kopii danych, administrator danych wydaje osobie kopię danych jej dotyczących i odnotowuje fakt wydania pierwszej kopii danych. Administrator danych może stosować cennik kopii danych, zgodnie z którym pobiera opłaty za kolejne kopie danych. Cenę kopii danych administrator danych kalkuluje w oparciu o szacowany jednostkowy koszt obsługi żądania wydania kopii danych.
- IX.2.5. Sprostowanie danych – w przypadku zgłoszenia przez osobę żądania dotyczącego jej praw w zakresie błędnych danych, administrator danych dokonuje sprostowania nieprawidłowych danych. Administrator danych ma prawo odmówić sprostowania danych, chyba że osoba w sposób racjonalny i przejrzysty wykaże nieprawidłowości danych, których sprostowania się domaga. W przypadku dokonania sprostowania danych, administrator na żądanie osoby, informuje ją o odbiorcach jej danych.
- IX.2.6. Uzupełnienie danych – w przypadku zgłoszenia przez osobę żądania dotyczącego jej praw w zakresie uzupełnienia danych, administrator danych aktualizuje i uzupełnia dane. Administratorowi przysługuje prawo odmowy uzupełnienia danych, jeżeli takie działanie pozostawałoby w sprzeczności z celem przetwarzania danych. W zakresie uzupełnienia danych, administrator może polegać na oświadczeniu osoby, chyba że oświadczenie to okaże się niewystarczające w świetle przyjętych przez administratora danych procedur, prawa lub zaistnienia podstaw, aby uznać oświadczenie za niewiarygodne.
- IX.2.7. Ograniczenie przetwarzania – Administrator danych ogranicza przetwarzanie danych osobowych w przypadku żądania osoby, gdy: (a) podważa ona prawidłowość danych – przez czas, w którym administrator dokonuje sprawdzenia poprawności danych, (b) przetwarzanie danych jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania, (c) dane przetwarzane przez administratora nie są już potrzebne, dla celów w jakich zostały zebrane, jednak są potrzebne osobie, której dane dotyczą, w związku z działaniem tej osoby w zakresie ustalenia, dochodzenia, albo też obrony roszczeń, (d) w związku z jej szczególną sytuacją, osoba wniosła sprzeciw w stosunku do przetwarzania przez administratora dotyczących tej osoby danych – do czasu stwierdzenia, czy po stronie administratora zachodzą prawnie uzasadnione podstawy nadrzędne, wobec podstaw sprzeciwu.
- IX.2.8. Usunięcie danych – w przypadku zgłoszenia przez osobę żądania dotyczącego jej praw w zakresie usunięcia danych, administrator danych usuwa dane: (a) które są zbędne dla celów, dla których zostały zebrane, (b) co do których została cofnięta zgoda na ich przetwarzanie i nie istnieje inna podstawa przetwarzania, (c) co do których osoba wniosła skuteczny sprzeciw w zakresie ich przetwarzania, (d) które były przetwarzane sprzecznie z podstawą prawną, (e) których przymus

usunięcia wynika z obowiązku prawnego, (f) które dotyczą danych dziecka zebranych na podstawie wcześniejszej zgody.

IX.2.9. Przenoszenie danych – administrator danych na żądanie osoby wydaje w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego lub przekazuje innemu podmiotowi, jeśli jest to możliwe, dane dotyczące tej osoby, które dostarczyła ona administratorowi, przetwarzane na podstawie zgody tej osoby lub w celu zawarcia lub wykonania umowy z nią zawartej, w systemach informatycznych administratora danych.

IX.2.10. Prawo do sprzeciwu – w przypadku zgłoszenia przez osobę żądania dotyczącego jej praw, w postaci umotywowanego szczególną sytuacją sprzeciwu, co do przetwarzania dotyczących tej osoby danych, a dane przetwarzane są przez administratora w oparciu o jego uzasadniony interes lub w oparciu o powierzone administratorowi zadanie realizowane w interesie publicznym, administrator danych uwzględni sprzeciw, przy zastrzeżeniu, że nie zachodzą po stronie administratora ważne, prawnie uzasadnione podstawy do przetwarzania, mające skutek nadrzędny w stosunku do interesów, praw i wolności osoby zgłaszającej sprzeciw, albo też podstawy do ustalenia, dochodzenia lub obrony roszczeń.

IX.2.11. Badania naukowe, historyczne lub dla celów statystycznych – w przypadku zgłoszenia przez osobę żądania dotyczącego jej praw w sytuacji, gdy administrator danych przetwarza dane w związku z prowadzonymi badaniami naukowymi, historycznym albo też przetwarza dane w celach statystycznych, w postaci umotywowanego szczególną sytuacją sprzeciwu w stosunku do takiego przetwarzania, administrator uwzględni taki sprzeciw, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym.

IX.2.12. Marketing bezpośredni – w przypadku zgłoszenia przez osobę żądania dotyczącego jej praw w sytuacji, gdy administrator danych przetwarza dane na potrzeby marketingu bezpośredniego (w tym ewentualnie profilowania), administrator uwzględni sprzeciw i zaprzestanie takiego przetwarzania.

IX.2.13. Prawa osób trzecich – administrator danych realizując prawa osób, których dane dotyczą, wprowadza proceduralne gwarancje ochrony praw i wolności osób trzecich. W szczególności w przypadku powzięcia wiarygodnej wiadomości o tym, że wykonanie żądania osoby o wydanie kopii danych lub prawa do przeniesienia danych może niekorzystnie wpłynąć na prawa i wolności innych osób (np. prawa związane z ochroną danych innych osób, prawa własności intelektualnej, tajemnicę handlową, dobra osobiste itp.), administrator może zwrócić się do osoby w celu wyjaśnienia wątpliwości lub podjąć inne prawem dozwolone kroki, łącznie z odmową zadośćuczynienia żądaniu.

IX.2.14. Prawo do ludzkiej interwencji przy automatycznym przetwarzaniu – jeżeli administrator przetwarza dane w sposób automatyczny, w tym w szczególności profiluje osoby, i w konsekwencji podejmuje względem osoby decyzje wywołujące skutki prawne, albo też inaczej skutki istotnie wpływające na osobę, Podmiot danych zapewnia możliwość odwołania się do interwencji i decyzji człowieka po stronie Spółki, chyba że taka automatyczna decyzja (a) jest niezbędna do zawarcia lub wykonania umowy między odwołującą się osobą a administratorem lub (b) jest wprost dozwolona przepisami prawa, albo też (c) opiera się o wyraźną zgodę odwołującej osoby.

IX.3 Obowiązki informacyjne

IX.3.1. W ramach obowiązków informacyjnych administrator danych określa sposoby wykonywania obowiązków informacyjnych, nając na uwadze zgodność z prawem i efektywność tych sposobów.

IX.3.2. W ramach obowiązków informacyjnych administrator danych w każdym przypadku, gdy jest to możliwe, określa sposób informowania osób o przetwarzaniu danych niezidentyfikowanych.

IX.3.3. W ramach obowiązków informacyjnych administrator danych jeżeli nie wymaga to niewspółmiernie dużego wysiłku oraz jest możliwe, informuje odbiorców danych o sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych.

IX.3.4. W ramach obowiązków informacyjnych administrator danych nie później niż przy pierwszym kontakcie z osobą, informuje tą osobę o prawie przysługującego jej sprzeciwu w stosunku do przetwarzania danych przez administratora.

IX.3.5. W ramach obowiązków informacyjnych administrator danych bez zbędnej zwłoki zawiadamia osobę o naruszeniu ochrony danych osobowych, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności tej osoby.

- IX.3.6. W ramach obowiązków informacyjnych administrator danych po otrzymaniu żądania od osoby, którego to żądania nie może spełnić w terminie wskazanym w RODO, informuje osobę o przedłużeniu ponad jeden miesiąc terminu na rozpatrzenie jej żądania.
- IX.3.7. W ramach obowiązków informacyjnych administrator danych, w przypadku pozyskania danych od osoby trzeciej, informuje konkretną osobę o przetwarzaniu jej danych, których nie pozyskał bezpośrednio od niej.
- IX.3.8. W ramach obowiązków informacyjnych administrator danych informuje osobę o przetwarzaniu jej danych, które pozyskał bezpośrednio od tej osoby.
- IX.3.9. W ramach obowiązków informacyjnych administrator danych, winien poinformować każdą osobę o planowanej zmianie celu przetwarzania dotyczących jej danych.
- IX.3.10. W ramach obowiązków informacyjnych administrator danych w przypadku uchylenia ograniczenia przetwarzania, informuje osobę przed uchyleniem ograniczenia przetwarzania.

X. ZAPEWNIENIE BEZPIECZEŃSTWA DANYCH

Administrator danych zapewnia bezpieczeństwo danych, które odpowiada ryzyku naruszenia praw i wolności osób fizycznych, związanego z przetwarzaniem danych osobowych przez administratora. Celem realizacji zasady bezpieczeństwa danych, administrator dokonuje:

- X.1.** Analizy ryzyka i adekwatności środków bezpieczeństwa – administrator przeprowadza i dokumentuje analizy adekwatności środków bezpieczeństwa danych osobowych. W tym celu administrator wewnętrznie lub ze wsparciem podmiotów wyspecjalizowanych (a) zapewnia odpowiedni stan wiedzy o bezpieczeństwie informacji, cyberbezpieczeństwie i ciągłości działania, (b) kategoryzuje dane oraz czynności przetwarzania pod kątem ryzyka, (c) analizuje ryzyko naruszenia praw lub wolności osób fizycznych w wyniku przetwarzania danych osobowych. Administrator winien dokonać analizy wszystkich możliwości naruszenia ochrony danych osobowych, biorąc pod uwagę cele przetwarzania, i związane z tym ryzyko naruszenia praw lub wolności osób fizycznych, (d) ustala możliwe do zastosowania techniczne i organizacyjne środki bezpieczeństwa z jednoczesną oceną kosztów ich wdrożenia.
- X.2.** Środki bezpieczeństwa – administrator danych stosuje środki bezpieczeństwa ustalone w ramach analiz ryzyka i adekwatności środków bezpieczeństwa oraz ocen skutków dla ochrony danych. Środki bezpieczeństwa danych osobowych, stanowią element środków bezpieczeństwa informacji i zapewnienia cyberbezpieczeństwa. Zostały one opisane w polityce bezpieczeństwa przetwarzania danych oraz procedurze 2, dotyczącej zapewnienia bezpieczeństwa przetwarzania danych osobowych.
- X.3.** Oceny skutków dla ochrony danych – administrator danych powinien dokonać oceny skutków planowanych operacji przetwarzania danych dla ochrony danych osobowych w każdym przypadku, w którym zgodnie z analizą ryzyka, ryzyko naruszenia praw i wolności osób fizycznych jest wysokie.
- X.4.** Zgłaszanie naruszeń – administrator danych, wdrożył i stosuje odpowiednią procedurę 5, pozwalającą na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych, Urzędowi Ochrony Danych w terminie 72 godzin od ustalenia naruszenia.

XI. PRZETWARZAJĄCY

Administrator danych winien stosować zasady doboru i weryfikacji przetwarzających dane na jego rzecz. Zasady doboru i weryfikacji muszą być opracowane w celu zapewnienia, aby przetwarzający dane na rzecz administratora, dawali wystarczające gwarancje wdrożenia odpowiednich środków organizacyjnych i technicznych, które zapewnią bezpieczeństwo, dla realizacji praw jednostki i innych obowiązków ochrony danych spoczywających na administratorze danych.

XII. PROCEDURY

Załącznikiem do niniejszego PODO są procedury:

PROCEDURA 1 – OCENA SKUTKÓW DLA OCHRONY DANYCH OSOBOWYCH,

PROCEDURA 2 – ZAPEWNIENIE BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH,

PROCEDURA 3 – POWOŁANIE INSPEKTORA OCHRONY DANYCH OSOBOWYCH,

PROCEDURA 4 – REJESTROWANIE CZYNNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH,

PROCEDURA 5 – ZGŁOSZENIE NARUSZENIA OCHRONY DANYCH OSOBOWYCH ORGANOWI NADZORCZEMU,

PROCEDURA 6 – OBOWIĄZEK INFORMACYJNY PRZY GROMADZENIU DANYCH OSOBOWYCH,

PROCEDURA 7 – ŻĄDANIE DOSTĘPU DO DANYCH OSOBOWYCH,

PROCEDURA 8 – ZAWIADOMIENIE OSOBY, KTÓREJ DANE DOTYCZĄ O NARUSZENIU OCHRONY DANYCH OSOBOWYCH,

PROCEDURA 9 – SPRZECIW WOBEC PRZETWARZANIA DANYCH OSOBOWYCH,

PROCEDURA 10 – ŻĄDANIE SPROSTOWANIA LUB UZUPEŁNIENIA DANYCH OSOBOWYCH,

PROCEDURA 11 – ŻĄDANIE OGRANICZENIA PRZETWARZANIA DANYCH OSOBOWYCH,

PROCEDURA 12 – ŻĄDANIE PRZENIESIENIA DANYCH OSOBOWYCH, PROCEDURA 13 – ŻĄDANIE USUNIĘCIA DANYCH OSOBOWYCH.

