POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH W TOM MEDIA SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

tel.: 32 765 00 50, 32 444 50 00; bok@tvtom.pl ; www.tvtom.pl ; /tommedia.tv
NIP: 6292465423, *REGON:* 243069532, KRS: 0000435008

SPIS TREŚCI

tel.: 32 765 00 50, 32 444 50 00; bok@tvtom.pl ; www.tvtom.pl ; /tommedia.tv
NIP: 6292465423, *REGON:* 243069532, KRS: 0000435008

WSTĘP. POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

Procedura Polityki Bezpieczeństwa Danych Osobowych zawarta w niniejszym dokumencie została opracowana w oparciu o wymagania zawarte w Rozporządzeniu Parlamentu Europejskiego i Rady (dalej RODO) /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 /Dz. Urz. UE. L nr 119, str.1/, Dokument zawiera sposób przygotowania i zbiór dokumentacji opisującej politykę bezpieczeństwa w zakresie odnoszącym się do sposobu przetwarzania danych osobowych oraz środków ich ochrony określonych w rozporządzeniu. Rozporządzenie RODO wiąże w całości, jest stosowane bezpośrednio i nie wymaga przystosowania do porządków krajowych poszczególnych państw, dlatego jest instrumentem pozwalającym na silniejsze zbliżenie prawa, kompleksowo regulując ochronę danych osobowych w Unii Europejskiej. Kreując politykę bezpieczeństwa przetwarzania danych, RODO zakłada indywidualne podejście w tej kwestii każdego przedsiębiorstwa w celu wdrożenia niezbędnych zabezpieczeń, które spełnią wymogi RODO i będą skutecznie chronić prawa osób. W tym celu konieczne jest uwzględnienie poziomu wiedzy na temat zabezpieczeń technicznych, zakresu i celów przetwarzania, ryzyka naruszenia praw lub wolności osób fizycznych wynikających z przetwarzania. Administrator Danych Osobowych (dalej: Administrator) na podstawie zebranych danych, odpowiedzialny jest za wdrożenie odpowiednich środków technicznych i organizacyjnych, zarówno przy określeniu sposobów przetwarzania, jak i w czasie samego przetwarzania.

Istotne jest też budowanie świadomości pracowników, postępowanie zgodnie z przyjętymi zasadami, raportowanie zagrożeń i incydentów, regularny udział w szkoleniach z zakresu ochrony danych osobowych oraz bezpieczeństwa informacji oraz reagowanie na zmieniające się otoczenie wewnętrzne i zewnętrzne w firmie.

W celu ochrony danych osobowych Administratorzy danych (firmy, organizacje itp.) powinni zorganizować odpowiednią strukturę oraz wdrożyć zabezpieczenia techniczne i organizacyjne dla skutecznego zarządzania bezpieczeństwem danych osobowych.

O tych właśnie zagadnieniach mówi Polityka bezpieczeństwa przetwarzania danych osobowych.

1. POSTANOWIENIA OGÓLNE

1.1. Artykuł 24 RODO zobowiązuje Administratora do wdrożenia odpowiednich środków technicznych i organizacyjnych realizujących wytyczne RODO poprzez wdrażaniu środków gwarantujących organizacyjne i techniczne bezpieczeństwo przetwarzania danych osobowych

1.2. Celem Polityki Bezpieczeństwa Przetwarzania Danych Osobowych, zwanej dalej „Polityką bezpieczeństwa" w TOM MEDIA SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ, zwanej dalej „Administratorem", jest zapewnienie ochrony danych osobowych przetwarzanych przez Administratora przed wszelakiego rodzaju zagrożeniami, tak wewnętrznymi jak i zewnętrznymi, świadomymi lub nieświadomymi.

1.3. Celem Polityki Bezpieczeństwa jest wskazanie działań jakie należy wykonać oraz ustanowienie zasad i reguł postępowania, które należy stosować, aby właściwie zabezpieczać dane osobowe. Podstawowe z tych działań to organizacyjne, fizyczne i logiczne zabezpieczenie posiadanych danych osobowych oraz edukowanie użytkowników systemu ochrony danych osobowych.

1.4. Polityka Bezpieczeństwa dotyczy zadań związanych z zabezpieczeniem danych osobowych zarówno przetwarzanych w sposób tradycyjny (wersje papierowe) jak i w systemach informatycznych. Osoby mające kontakt z zbiorami zawierającymi dane osobowe zobowiązane są do przestrzegania postanowień Polityki Bezpieczeństwa.

1.5. Niniejsza Polityka Bezpieczeństwa opisuje w szczególności zasady postepowania przy przetwarzaniu danych osobowych i ich zabezpieczenia przed nieuprawnionym dostępem.

1.6. Stosowanie zasad określonych w niniejszym dokumencie ma na celu zapewnienie bezpieczeństwa danych osobowych, przetwarzanych przez TOM MEDIA SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ rozumianej jako ochronę danych przed ich udostępnieniem osobom nieupoważnionym, zmianą lub zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem Ustawy oraz utratą, uszkodzeniem lub zniszczeniem.

1.7. Polityka Bezpieczeństwa przetwarzania danych osobowych realizowana jest poprzez zabezpieczenia fizyczne, organizacyjne, oprogramowanie systemowe, aplikacje oraz użytkowników proporcjonalne

tel.: 32 765 00 50, 32 444 50 00; bok@tvtom.pl ; www.tvtom.pl ; /tommedia.tv
NIP: 6292465423, *REGON:* 243069532, KRS: 0000435008

i adekwatne do ryzyka naruszenia bezpieczeństwa danych osobowych przetwarzanych w ramach prowadzonej działalności.

1.8. Administratorem przetwarzanych danych osobowych jest TOM MEDIA SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ.

1.9. Administrator powołał/ nie powołał/* inspektora ochrony danych, zgodnie art. 37 RODO. Wzór dokumentu powołania stanowi Załącznik Nr 1.

1.10. Dopuszcza się powołanie jednego wspólnego inspektora ochrony danych dla grupy przedsiębiorstw pod warunkiem spełnienia warunków określonych w art. 37 RODO. Zadania inspektora ochrony danych zawarte są w art. 39 RODO.

1.11. Obszarem przetwarzania danych osobowych przez TOM MEDIA SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ jest każdorazowy adres siedziby Administratora.

1.12. Utrzymanie bezpieczeństwa przetwarzanych danych osobowych w TOM MEDIA SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ rozumiane jest jako zapewnienie ich poufności, integralności, rozliczalności oraz dostępności na odpowiednim poziomie. Miarą bezpieczeństwa przetwarzanych danych osobowych jest akceptowalna wielkość ryzyka związanego z ochroną przetwarzanych danych.

1.13. Zastosowane zabezpieczenia jakie podejmuje Administrator mają służyć osiągnięciu bezpieczeństwa przetwarzanych danych i zapewnić:

1.13.1. poufność danych – polega na zapewnieniu, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, podmiotom lub procesom.

1.13.2. integralność danych – rozumianą jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;

1.13.3. rozliczalność danych – oznaczającą, że działania osób mogą być przypisane w sposób jednoznaczny tylko tym osobom,

1.13.4. autentyczność –polegająca na zapewnieniu, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana (autentyczność dotyczy użytkowników, procesów, systemów i informacji),

1.13.5. integralność systemu – co oznacza, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej przy systemach operacyjnych,

1.13.6. dostępność informacji – zapewnienie osoby upoważnionym dostępu do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne,

1.13.7. braku możliwości wyparcia się swego uczestnictwa w całości lub w części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie,

1.13.8. zarządzanie ryzykiem – rozumiane jako proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych służących do przetwarzania danych osobowych.

2. DEFINICJE

2.1. Przez użyte w Polityce Bezpieczeństwa określenia zgodnie z art. 4 RODO należy rozumieć:

2.1.1. administrator danych osobowych – zgodnie z art. 4 ust. 7 RODO, jest to osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych,

2.1.2. inspektor ochrony danych – – zgodnie z art. 37 ust. 1 RODO, jest to osoba wyznaczona przez administratora danych osobowych, nadzorująca przestrzeganie zasad i wymogów ochrony danych osobowych określonych w RODO i przepisach krajowych,

2.1.3. RODO – 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 /Dz. Urz. UE.L nr 119, str. 1/,

2.1.4. dane osobowe – zgodnie z art. 4 ust. 1 RODO, są to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej,

2.1.5. zbiór danych osobowych – zgodnie z art. 4 ust. 6 RODO, jest to uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów,

tel.: 32 765 00 50, 32 444 50 00; bok@tvtom.pl ; www.tvtom.pl ; /tommedia.tv
NIP: 6292465423, *REGON:* 243069532, KRS: 0000435008

2.1.6. przetwarzane danych – zgodnie z art. 4 ust. 2, są to operacje lub zestaw operacji wykonywanych na danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, łączenie, przesyłanie, zmienianie, udostępnianie i usuwanie, niszczenie, itd.

2.1.7. system informatyczny – jest **zestaw** urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych, współpracujących ze sobą w celu przetwarzania danych osobowych,

2.1.8. system tradycyjny – to wyposażenie i środki trwałe wykorzystywane w celu przetwarzania danych osobowych na papierze,

2.1.9. zabezpieczenie danych w systemie informatycznym – to zapewnienie poprzez wdrożenie procedur i środków technicznych ochrony danych przed ich nieuprawnionym przetwarzaniem

2.1.10. administrator systemu informatycznego – osoba lub osoby, upoważnione przez administratora danych osobowych do administrowania i zarządzania systemami informatycznymi,

2.1.11. podmiot przetwarzający - zgodnie z art. 4 ust. 8 RODO osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, upoważniona przez administratora do przetwarzania danych w jego imieniu,

2.1.12. odbiorca – zgodnie z art. 4 ust. 9 RODO to osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe w oparciu m. in. o umowę powierzenia,

2.1.13. strona trzecia – zgodnie z art. 4 ust. 10 RODO to osoba fizyczna lub prawna, organ publiczny, jednostka lub podmiot inny niż osoba, której dane dotyczą, które z upoważnienia administratora danych osobowych mogą przetwarzać dane osobowe,

2.1.14. identyfikator użytkownika (login) – ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,

2.1.15. zgoda osoby – zgodnie z art. 4 ust. 11 RODO to świadome i dobrowolne okazanie woli,

2.1.16. hasło – ciąg znaków literowych, cyfrowych lub innych, przypisany do identyfikatora użytkownika, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.

3. OBOWIĄZEK INFORMACYJNY.

3.1. Zgodnie z art. 13 RODO w przypadku zbierania danych osobowych od osoby, której one dotyczą, w wypadkach przewidzianych Ustawą należy poinformować tę osobę o:

3.1.1. Pełnej nazwie Administratora i adresie siedziby,

3.1.2. Celu zbierania danych, a w szczególności o znanych w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych,

3.1.3. Prawie dostępu do swoich danych oraz ich poprawiania,

3.1.4. Dobrowolności lub obowiązku podania danych - jeżeli taki obowiązek istnieje, o jego podstawie prawnej.

3.1.5. Wzór Klauzuli Informacyjnej stanowi Załącznik Nr 2

4. WYKAZ ZBIORÓW DANYCH OSOBOWYCH

4.1. Zbiór danych osobowych to zbiór spełniający przesłanki: zawiera dane osobowe, ma określoną, własną strukturę oraz zapewnia dostęp do danych według określonych kryteriów. Za zbiór danych można uznać wszelkie materiały gromadzone w formie akt.

4.2. Dane osobowe gromadzone są w zbiorach :

4.2.1. Ewidencja osób upoważnionych do przetwarzania danych osobowych,

4.2.2. Akta osobowe pracowników – przykładowa struktura zbioru

4.2.2.1. Imię, nazwisko,
4.2.2.2. płeć,
4.2.2.3. pesel,
4.2.2.4. seria i numer dowodu,
4.2.2.5. Adres do korespondencji,

tel.: 32 765 00 50, 32 444 50 00; bok@tvtom.pl ; www.tvtom.pl ; /tommedia.tv
NIP: 6292465423, *REGON:* 243069532, KRS: 0000435008

4.2.2.6. urząd skarbowy,
4.2.2.7. data urodzenia

4.2.3. Zbiory informacji o pracownikach, oświadczenia na potrzeby ZFŚS,
4.2.4. Ewidencja zwolnień lekarskich,
4.2.5. Skierowania na badania okresowe, specjalistyczne,
4.2.6. Ewidencja urlopów, czasu pracy, wyjść,
4.2.7. Kartoteki wydanej odzieży ochronnej i środków ochrony indywidualnej,
4.2.8. Rejestr delegacji służbowych,
4.2.9. Listy płac pracowników,
4.2.10. Deklaracje ubezpieczeniowe pracowników,
4.2.11. Deklaracje i kartoteki ZUS pracowników,
4.2.12. Deklaracje podatkowe pracowników,
4.2.13. Rejestr wypadków,
4.2.14. Umowy cywilno-prawne,
4.2.15. Umowy zawierane z kontrahentami,
4.2.16. Rejestr klientów,
4.2.17. Dokumenty archiwalne,

5. ZAKRES STOSOWANIA

5.1. TOM MEDIA SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ jako Administrator przetwarza dane osobowe: pracowników, byłych pracowników, stażystów, klientów, kontrahentów, odbiorców danych osobowych, którym przekazano dane osobowe do przetwarzania w oparciu o umowy powierzenia Administratora oraz osób współpracujących na podstawie umów cywilnoprawnych, w tym danych osobowych i treści zawieranych umów.

5.2. Do przetwarzania danych administrator używa postaci dokumentacji tradycyjnej (papierowej) i w formie elektronicznej.

5.3. Polityka bezpieczeństwa zawiera uregulowania dotyczące wprowadzonych zabezpieczeń technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych.

5.4. TOM MEDIA SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ jako Administrator reguluje również ochronę danych osobowych za pomocą dodatkowych dokumentów jakimi są:

5.4.1. ewidencja osób upoważnionych do przetwarzania danych osobowych Załącznik Nr 4,
5.4.2. rejestr naruszeń Załącznik Nr 9,
5.4.3. rejestr czynności przetwarzania danych osobowych Załącznik Nr8,
5.4. 4. procedura postępowania w przypadku naruszenia ochrony danych osobowych.

5.5. Polityka Bezpieczeństwa dotyczy również wszystkich Informacji dotyczących zabezpieczenia danych osobowych, w tym w szczególności nazw kont i haseł w systemach przetwarzania danych osobowych oraz osób dopuszczonych do przetwarzania danych osobowych.

5.6. Polityka bezpieczeństwa określona jest również przez zasady bezpieczeństwa obowiązujące użytkowników przetwarzających dane osobowe, z którymi należy zapoznać użytkowników komputerów na których przetwarzane są te. Zbiór zasad stanowi Załącznik Nr 6.

5.7. Zakresy ochrony danych osobowych określone przez Politykę bezpieczeństwa oraz inne z nią związane dokumenty mają zastosowanie do:

5.7.1. wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz dokumentów papierowych, w których przetwarzane są dane osobowe podlegające ochronie,
5.7.2. wszystkich lokalizacji – budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie,
5.7.3. wszystkich pracowników, byłych pracowników, przyszłych pracowników, stażystów, i innych osób mających dostęp do informacji podlegających ochronie

tel.: 32 765 00 50, 32 444 50 00; bok@tvtom.pl ; www.tvtom.pl ; /tommedia.tv
NIP: 6292465423, *REGON:* 243069532, KRS: 0000435008

6. OBOWIĄZKI I ODPOWIEDZIALNOŚĆ ADMINISTRATORA

6.1. Do najważniejszych obowiązków Administratora należy:

6.1.1. Przetwarzanie danych osobowych wyłącznie w przypadkach, gdy spełniony jest co najmniej jeden z warunków określonych w art. 6 RODO,

6.1.2. Organizacja bezpieczeństwa i ochrony danych osobowych zgodnie z wymogami ustawy o ochronie danych osobowych oraz innych przepisów regulujących zasady bezpieczeństwa i ochrony danych osobowych,

6.1.3. Zapewnienie przetwarzania danych zgodnie z uregulowaniami Polityki Bezpieczeństwa,

6.1.4. Wydawanie i anulowanie upoważnień do przetwarzania danych osobowych,

6.1.5. Przeprowadzanie szkoleń użytkowników przed dopuszczeniem do pracy z systemem informatycznym przetwarzającym dane osobowe,

6.1.6. Prowadzenie ewidencji czynności przetworzenia danych osobowych,

6.1.7. Prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych;

6.1.8. Prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych,

6.1.9. Nadzór nad bezpieczeństwem danych osobowych,

6.1.10. Kontrola działań pracowników pod względem zgodności przetwarzania danych z przepisami o ochronie danych osobowych,

6.1.11. Inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych,

6.1.12. Bieżący monitoring i zapewnienie ciągłości działania systemu informatycznego oraz baz danych,

6.1.13. Optymalizacja wydajności systemu informatycznego, baz danych, instalacje I konfiguracje sprzętu sieciowego i serwerowego,

6.1.14. Instalacje i konfiguracje oprogramowania systemowego, sieciowego, oprogramowania bazodanowego,

6.1.15. Konfiguracja i administrowanie oprogramowaniem systemowym, sieciowym oraz bazodanowym zabezpieczającym dane chronione przed nieupoważnionym dostępem,

6.1.16. Współpraca z dostawcami usług oraz sprzętu sieciowego i serwerowego oraz zapewnienie zapisów dotyczących ochrony danych osobowych,

6.1.17. Zarządzanie kopiami awaryjnymi konfiguracji oprogramowania systemowego, sieciowego,

6.1.18. Przeciwdziałanie próbom naruszenia bezpieczeństwa informacji,

6.1.19. Zmiana lub usprawnienia procedur bezpieczeństwa i standardów zabezpieczeń,

6.1.20. Zarządzanie licencjami oraz procedurami ich dotyczącymi,

6.1.21. Prowadzenie profilaktyki antywirusowej.

6.2. Część zadań zakresu objętego ust. 1 p pkt 6.1.11 do 6.1.20 w przypadku braku w własnych działów informatycznych Administrator może powierzyć na podstawie umowy wraz z upoważnieniem do przetwarzania części danych osobowych, firmom informatycznym świadczącym obsługę informatyczną dla Administratora.

7. ZARZĄDZANIE OCHRONĄ DANYCH OSOBOWYCH.

7.1. Za bieżącą, operacyjną ochronę danych osobowych odpowiada każda osoba przetwarzająca te dane w zakresie zgodnym z upoważnieniem oraz rolą sprawowaną w procesie przetwarzania danych.

7.2. dostęp do danych osobowych powinien być przyznawany zgodnie z zasadą wiedzy koniecznej.

7.3. Każda z osób mająca styczność z danymi osobowymi jest zobowiązana do ochrony danych osobowych oraz przetwarzania ich w granicach udzielonego jej upoważnienia.

7.4. Należy zapewnić poufność, integralność i rozliczalność przetwarzanych danych osobowych.

7.5. Należy stosować adekwatny do zmieniających się warunków i technologii poziom bezpieczeństwa przetwarzania danych osobowych.

7.6. Dane osobowe powinny być chronione przed nieuprawnionym dostępem i modyfikacją.

7.7. Dane osobowe należy przetwarzać wyłącznie za pomocą autoryzowanych urządzeń służbowych.

tel.: 32 765 00 50, 32 444 50 00; bok@tvtom.pl ; www.tvtom.pl ; /tommedia.tv
NIP: 6292465423, *REGON:* 243069532, KRS: 0000435008

8.UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

8.1. Administrator jest obowiązany zapewnić kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane, czyli jednym z najważniejszych obowiązków administratora danych jest posiadanie wiedzy nad tym kto, kiedy i w jakim zakresie ma dostęp do jego zasobów chronionych.

8.2. Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez Administratora na mocy art. 28 RODO (Załącznik Nr 3).

8.3. Upoważnienia są wydawane indywidualnie przed rozpoczęciem przetwarzania danych osobowych przez Administratora.

8.4. W celu otrzymania przez Użytkownika upoważnienia do przetwarzania danych osobowych, należy dostarczyć do Administratora podpisane oświadczenie użytkownika.

8.5. Na podstawie otrzymanego oświadczenia Administrator upoważnia Użytkownika do przetwarzania danych osobowych i wydaje upoważnienie do przetwarzania danych osobowych. Upoważnienia, o których mowa powyżej przechowywane przez Administratora.

8.6. Upoważnienie może być w każdym czasie odwołane przez Administratora. Oświadczenie o odwołaniu upoważnienia do przetwarzania danych osobowych powinno być sporządzone na piśmie. Upoważnienie do przetwarzania danych osobowych wygasa z chwilą ustania przesłanki będącej podstawą wydania upoważnienia, w tym w szczególności wygaśnięcia stosunku pracy lub umowy cywilnoprawnej łączącej Użytkownika z Administratorem.

9. OBOWIĄZKI OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

9.1. Do najważniejszych obowiązków osób upoważnionych do przetwarzania danych osobowych należy:

9.1.1. Znajomość, zrozumienie i stosowanie w możliwie największym zakresie wszelkich dostępnych środków ochrony danych osobowych oraz uniemożliwienie osobom, nieuprawnionym dostępu do swojej stacji roboczej,

9.1.2. Przetwarzanie danych osobowych zgodnie z obowiązującymi przepisami prawa oraz przyjętymi regulacjami,

9.1.3. Prowadzenie rejestru czynności przetwarzania na zasadach określonych w art. 30 RODO. Wzór rejestru stanowi Załącznik Nr 8.

9.1.4. Postępowania zgodnie z ustalonymi regulacjami wewnętrznymi dotyczącymi przetwarzania danych osobowych,

9.1.5. Zachowania w tajemnicy danych osobowych, do których uzyskały dostęp oraz informacji o sposobach ich zabezpieczenia,

9.1.6. Ochrony danych osobowych oraz środków przetwarzających dane osobowe przed nieuprawnionym dostępem, ujawnieniem, modyfikacją, zniszczeniem lub zniekształceniem,

9.1.7. Informowania Administratora o wszelkich podejrzeniach naruszenia lub zauważonych naruszeniach oraz słabościach systemu przetwarzającego dane osobowe,

9.1.8. Zapoznanie się z Polityką Bezpieczeństwa przetwarzania danych osobowych oraz o ile funkcjonuje Instrukcją Zarządzania Systemem Informatycznym, służącym do przetwarzania danych osobowych.

10. EWIDENCJA OSÓB UPOWAŻNIONYCH.

10.1. Zgodnie z art. 39 RODO Administrator prowadzi ewidencję osób upoważnionych do ich przetwarzania, która powinna zawierać: imię i nazwisko osoby upoważnionej, datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych oraz identyfikator, jeżeli dane są przetwarzane w systemie informatycznym.

tel.: 32 765 00 50, 32 444 50 00; bok@tvtom.pl ; www.tvtom.pl ; /tommedia.tv
NIP: 6292465423, *REGON:* 243069532, KRS: 0000435008

10.2. Ewidencja osób upoważnionych do przetwarzania danych osobowych jest prowadzona przez Administratora zgodnie ze wzorem formularza stanowiącym Załącznik nr 4 do Polityki Bezpieczeństwa przetwarzania danych osobowych.

11.SZKOLENIA UŻYTKOWNIKÓW

11.1. Każdy użytkownik przed dopuszczeniem do pracy z systemem informatycznym przetwarzającym dane osobowe lub zbiorami danych osobowych w wersji papierowej winien być poddany przeszkoleniu w zakresie ochrony danych osobowych w zbiorach elektronicznych i papierowych.

11.2. Za przeprowadzenie szkolenia odpowiada Administrator.

11.3. Zakres szkolenia powinien obejmować zaznajomienie użytkownika z przepisami RODO, Polityką Bezpieczeństwa danych i Instrukcją Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych obowiązującymi u Administratora.

Po zaznajomieniu się z powyższymi regulacjami, użytkownik, przed dopuszczeniem do przetwarzania danych, powinien zobowiązać się do ich przestrzegania przez podpisanie oświadczenia użytkownika, stanowiącego Załącznik nr 3.

12. UDOSTĘPNIANIE DANYCH OSOBOWYCH.

12.1. Dane osobowe mogą być udostępniane wyłącznie podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa oraz osobom, których dotyczą,

12.2. Zgodnie z RODO udostępnienie danych może nastąpić:

12.2.1. z uwzględnieniem przepisów prawa,

12.2.2. w sytuacjach, gdy jest ono niezbędne do realizacji prawnie uzasadnionych celów administratora,

12.2.3. za wyraźną zgodą podmiotu, którego dane dotyczą.

12.3. Udostępnianie danych osobowych może nastąpić wyłącznie za zgodą Administratora.

12.4. Informacje zawierające dane osobowe powinny być przekazywane uprawnionym podmiotom lub osobom za potwierdzeniem odbioru listem poleconym za pokwitowaniem odbioru lub innym bezpiecznym sposobem, określonym wymogiem prawnym lub umową.

12.5. Udostępniając dane osobowe, należy zaznaczyć, że można je wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.

13. PROGRAMY INFORMATYCZNE WYKORZYSTYWANE DO PRZETWARZANIA DANYCH.

13.1. Do przetwarzania danych osobowych w TOM MEDIA SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ wykorzystywane są programy informatyczne wg Załącznika Nr 11.

13.2. Programy te posiadają licencje na użytkowanie i są aktualizowane zgodnie z informacją od dostawców.

13.3. Programy umieszczone są na serwerze w pomieszczeniu zamkniętym i chronionym.

13.4. Dostęp do serwera z komputerów użytkowników odbywa się za pomocą sieci zabezpieczonej przed nieuprawnionym dostępem.

14. POWIERZENIE DO PRZETWARZANIA.

14.1. Administrator może powierzyć dane osobowe do przetworzenia zewnętrznym firmom świadczącym wyspecjalizowane usługi kadrowe, księgowe czy też informatyczne. Zawarcie Umowy powierzenia wymaga formy pisemnej. Wzór Załącznik Nr 7.

14.2. Zgodnie z art. 28 ust. 1 RODO Administrator powinien korzystać wyłącznie z usług podmiotów, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą.

tel.: 32 765 00 50, 32 444 50 00; bok@tvtom.pl ; www.tvtom.pl ; /tommedia.tv
NIP: 6292465423, *REGON:* 243069532, KRS: 0000435008

14.3. Umowa powierzenia (Załącznik Nr 7) powinna zawierać następujące elementy
- **14.3.1.** przedmiot przetwarzania,
- **14.3.2.** czas trwania przetwarzania,
- **14.3.3.** charakter i cel przetwarzania,
- **14.3.4.** rodzaj danych osobowych,
- **14.3.5.** kategorię osób, których dane dotyczą,
- **14.3.6.** obowiązki i prawa administratora,
- **14.3.7.** obowiązki podmiotu przetwarzającego.

15. BEZPIECZEŃSTWO USŁUG ZEWNĘTRZNYCH.

15.1. Należy zapewnić aby usługi zewnętrzne były prowadzone wyłącznie zgodnie z wymaganiami bezpieczeństwa przetwarzania danych osobowych obowiązującymi w TOM MEDIA SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ, wymaganiami umowy oraz wymaganiami prawa.

15.2. Wymagania bezpieczeństwa przetwarzania danych osobowych, zakres usług oraz poziom ich dostarczania należy określić w umowie świadczenia usług.

15.3. Należy zapewnić aby użytkownicy nie będący pracownikami NAZWA FIRMY stosowali te same zasady bezpieczeństwa przetwarzania danych osobowych co użytkownicy będący pracownikami.

16. ŚRODKI ORGANIZACYJNE I TECHNICZNE ZABEZPIECZENIA PRZETWARZANIA DANYCH OSOBOWYCH.

16.1 Dane osobowe mogą być przetwarzane wyłącznie w obszarze przetwarzania danych osobowych, na które składają się pomieszczenia biurowe w siedzibie Administratora, z wyjątkiem sytuacji udostępnienia danych osobowych lub powierzenia przetwarzania danych osobowych. Szczegółowy wykaz pomieszczeń tworzących obszar przetwarzania danych osobowych znajduje się w Załączniku nr 10 do Polityki Bezpieczeństwa.

16.2 Dane osobowe Administrator przetwarza przy zastosowaniu zabezpieczeń zapewniających ich ochronę w postaci środków organizacyjnych, technicznych i środków ochrony fizycznej.

16.3 Dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych stosuje się następujące środki:

16.3.1 Środki organizacyjne:
- wdrożenie Polityki bezpieczeństwa przetwarzania danych osobowych oraz Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych,
- ustalona, indywidualna procedura udzielania upoważnień przez Administratora poprzedzonego szkoleniem z zakresu przepisów i zasad ochrony danych osobowych,
- prowadzenie ewidencji osób uprawnionych do przetwarzania danych osobowych, procedura postępowania w sytuacji naruszenia ochrony danych osobowych, konieczność składania deklaracji poufności przez Użytkowników danych, procedury przechowywania zbiorów danych.

16.3.2 Środki techniczne:
- zbiory danych osobowych przetwarzane są wyłącznie na autoryzowanym sprzęcie służbowym,
- stacje robocze wyposażone są w indywidualną ochronę antywirusową;
- dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.

16.3.3 Środki ochrony fizycznej:
- pomieszczenia, w których znajdują się zbiory danych osobowych, są zamykane na klucz, a dostęp do nich odbywa się wyłącznie w obecności pracowników Administratora,
- pomieszczenia, w którym przetwarzany jest zbiór danych osobowych znajdują się wewnątrz budynku w strefie ograniczonego dostępu,

tel.: 32 765 00 50, 32 444 50 00; bok@tvtom.pl ; www.tvtom.pl ; /tommedia.tv
NIP: 6292465423, *REGON:* 243069532, KRS: 0000435008

- zbiór danych osobowych w formie papierowej przechowywany jest w zamkniętej metalowej szafie,
- dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek.

17. OCHRONA DANYCH OSOBOWYCH W KORESPONDENCJI ELEKTRONICZNEJ

17.1 Korespondencja, która zawiera dane osobowe, powinna być przesyłana w formie zaszyfrowanego pliku, natomiast hasło przekazywać innym kanałem komunikacyjnym. Praktyka ta ma zapobiec sytuacji, w której wysyłamy dane osobowe w treści wiadomości e-mail i podczas wyboru adresata mylimy się, co skutkuje wysłaniem wiadomości do osoby nieuprawnionej do jej otrzymania.

17.2 Mechanizmem, który może uchronić użytkownika przed mylnym wyborem adresata jest wyłączenie funkcji podpowiadania adresu e-mail – oczywiście jest to pewnego rodzaju utrudnienie, ponieważ przy adresowaniu każdej wiadomości musimy wprowadzić cały adres e-mail, jednak mechanizm ten bardzo często uchroni nas przed wyborem nieodpowiedniego adresata.

17.3 Wysyłka korespondencji masowej do wielu adresatów wymaga ukrycia adresów odbiorców. Jeżeli tego nie zrobimy wszyscy odbiorcy będą widzieli adresy e-mail pozostałych osób. Taka sytuacja doprowadza do masowego upublicznienia danych osobowych .W przypadku wysyłania korespondencji masowej np. newsletter należy skorzystać z opcji „UDW" (kopia ukryta), która zapobiegnie wystąpieniu incydentu.

18.NISZCZEIE DOKUMENTACJI PAPIEROWEJ I W FORMIE ZAPISU ELEKTRONICZNEGO NA DYSKU KOMPUTERÓW I URZĄDZEŃ PRZENOŚNYCH.

18.1. Zgodnie art. 5 lit e dane osobowe powinny być przechowywane przez okres nie dłuższy niż jest to niezbędne do celów, w których dane są przetwarzane.

18.2. RODO zaostrza przepisy dotyczące niszczenia dokumentów.

18.3. Dokumenty zawierające dane osobowe w formie papierowej maja być niszczone w niszczarkach mechanicznych posiadających urządzenia tnące uniemożliwiające odczyt zniszczonych dokumentów lub mogą przekazywane do niszczenia firmom zewnętrznym gwarantującym ochronę przekazanych danych osobowych

18.4. i profesjonalizm.

18.5. Dane na komputerach i urządzeniach przenośnych typu laptopy, smartfony, mają być usuwane z pamięci dysków. Za pomocą przebijaka do dysku twardego można zniszczyć niepotrzebne dane elektroniczne bezpiecznie, wygodnie i niezawodnie.

18.6. Chcąc zminimalizować ryzyko utraty danych z pamięci USB zaleca się dopuszczanie do użytkowania przez pracowników jedynie firmowych pamięci USB, które są zaszyfrowane.

19. POSTĘPOWANIE W SYTUACJI NARUSZENIA BEZPIECZEŃSTWA DANYCH OSOBOWYCH.

19.1. Każdy użytkownik w przypadku stwierdzenia lub podejrzenia stwierdzenia zagrożenia lub naruszenia ochrony danych osobowych, zobowiązany jest o tym poinformować Administratora Danych.

19.2. Do typowych zagrożeń bezpieczeństwa danych osobowych należą:

19.2.1. Niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów;

19.2.2. Niewłaściwe zabezpieczenie sprzętu, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych;

19.2.3. Nieprzestrzeganie zasad ochrony danych osobowych przez pracowników.

19.3. Do typowych incydentów bezpieczeństwa danych osobowych należą:

19.3.1. Zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności),

tel.: 32 765 00 50, 32 444 50 00; bok@tvtom.pl ; www.tvtom.pl ; /tommedia.tv
NIP: 6292465423, *REGON:* 243069532, KRS: 0000435008

19.3.2. Zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata/ zagubienie danych);,

19.3.3. Umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania).

19.4. W przypadku stwierdzenia wystąpienia zagrożenia, Administrator Danych uruchamia Procedurę i prowadzi postępowanie wyjaśniające w toku którego:

19.4.1. Ustala zakres i przyczyny zagrożenia oraz jego ewentualne skutki,

19.4.2. Inicjuje ewentualne działania dyscyplinarne,

19.4.3. Rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych zagrożeń w przyszłości,

19.4.4. Dokumentuje prowadzone postępowania.

19.5. W przypadku stwierdzenia incydentu (naruszenia), Administrator Danych prowadzi postępowanie wyjaśniające, w toku którego:

19.5.1. Ustala czas wystąpienia naruszenia, jego zakres, przyczyny, skutki oraz wielkość szkód, które zaistniały,

19.5.2. Zabezpiecza ewentualne dowody;

19.5.3. Ustala osoby odpowiedzialne za naruszenie;

19.5.4. Podejmuje działania naprawcze (usuwa skutki incydentu i ogranicza szkody);

19.5.5. Inicjuje działania dyscyplinarne;

19.5.6. Wyciąga wnioski i rekomenduje działania korygujące zmierzające do eliminacji podobnych incydentów w przyszłości;

19.5.7. Dokumentuje prowadzone postępowania zgodnie ze wzorem Raportu z naruszenia bezpieczeństwa danych osobowych stanowiących Załącznik nr 9 do Polityki Bezpieczeństwa.

20. ZGODNOŚĆ POLITYKI BEZPIECZEŃSTWA PRZETWARZANIA DANYCH Z AKTUALNYM STANEM PRAWNYM.

20.1. Niniejsza Polityka powinna być aktualizowana wraz ze zmieniającymi się przepisami prawnymi o ochronie danych osobowych oraz zmianami faktycznymi w ramach TOM MEDIA SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ, które mogą powodować, że zasady ochrony danych osobowych określone w obowiązujących dokumentach będą nieaktualne lub nieadekwatne.

20.2. Administrator raz w roku sprawdza zgodność przetwarzania danych osobowych z przepisami o ochronie danych osobowych.

20.3. Okresowy przegląd Polityki Bezpieczeństwa powinien mieć na celu stwierdzenie, czy postanowienia Polityki odpowiadają aktualnej i planowanej działalności Administratora oraz stanowi prawnemu aktualnemu w momencie dokonywania przeglądu.

21. POSTANOWIENIA KOŃCOWE.

21.1. Administrator ma obowiązek zapoznać z treścią Polityki Bezpieczeństwa każdego użytkownika przetwarzającego dane osobowe.

21.2. Wszystkie regulacje dotyczące systemów informatycznych, określone w Polityce dotyczą również przetwarzania danych osobowych w bazach prowadzonych w jakiejkolwiek innej formie.

21.3. Użytkownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w Polityce.

21.4. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także, gdy nie

tel.: 32 765 00 50, 32 444 50 00; bok@tvtom.pl ; www.tvtom.pl ; /tommedia.tv
NIP: 6292465423, *REGON:* 243069532, KRS: 0000435008

zrealizowała stosownego działania dokumentującego ten przypadek, można wszcząć postępowanie dyscyplinarne.

21.5. Kara dyscyplinarna orzeczona wobec osoby uchylającej się od powiadomienia nie wyklucza odpowiedzialności karnej tej osoby, zgodnie z ustawą oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.

21.6. W sprawach nieuregulowanych w Polityce mają zastosowanie przepisy ustawy oraz rozporządzenia.

tel.: 32 765 00 50, 32 444 50 00; bok@tvtom.pl ; www.tvtom.pl ; /tommedia.tv
NIP: 6292465423, *REGON:* 243069532, KRS: 0000435008