

**POLITYKA BEZPIECZEŃSTWA
W ZAKRESIE OCHRONY DANYCH OSOBOWYCH
firmy Emm Consulting**

- I. **Mariusz Lasak – właściciel firmy świadomy wagi problemów związanych z ochroną prawa do prywatności, w tym w szczególności prawa osób fizycznych powierzających swoje dane osobowe dla właściwej i skutecznej ochrony tych danych deklaruje:**
1. zamiar podejmowania wszystkich działań niezbędnych dla ochrony praw i usprawiedliwionych interesów jednostki związanych z bezpieczeństwem danych osobowych,
 2. zamiar stałego podnoszenia świadomości oraz kwalifikacji osób przetwarzających dane osobowe w zakresie problematyki bezpieczeństwa tych danych,
 3. zamiar traktowania obowiązków osób zatrudnionych przy przetwarzaniu danych osobowych jako należących do kategorii podstawowych obowiązków pracowniczych, oraz stanowczego egzekwowania ich wykonania przez zatrudnione osoby,
 4. zamiar podejmowania w niezbędnym zakresie współpracy z instytucjami powołanymi do ochrony danych osobowych.
- II. Właściciel firmy świadomy jest zagrożenia związanego z przetwarzaniem danych osobowych na dużą skalę – w tym, w szczególności, z zagrożeń wynikających z dynamicznego rozwoju metod i technik przetwarzania tych danych w systemach informatycznych oraz sieciach telekomunikacyjnych. Deklaruje, że będzie stale doskonalił i rozwijał organizacyjne, techniczne oraz informatyczne środki ochrony danych osobowych przetwarzanych zarówno metodami tradycyjnymi jak i elektronicznie tak, aby skutecznie zapobiegać zagrożeniom:
- związanym z infekcjami wirusów i koni trojańskich, które instalując się na komputerze mogą wykraść zasoby tego komputera (zarówno stacjonarne jak i sieciowe),
 - związanym ze spamem, posiadającym niekiedy programy pozwalające wykraść zasoby komputera,
 - związanym z dostępem do stron internetowych, na części, których zainstalowane są skrypt pozwalające wykraść zasoby komputera,
 - związanym z ogólnie dostępnymi komunikatorami internetowymi, w których występują luki, przez które można uzyskać dostęp do komputera,
 - związanym z użytkowaniem oprogramowania do wymiany plików, mogącym służyć do łatwego skopiowania pliku,
 - związanym z możliwością niekontrolowanego kopiowania danych na zewnętrzne, przenośne nośniki,
 - związanym z możliwością podsłuchiwanie sieci, dzięki któremu można zdobyć hasła i skopiować objęte ochrona dane,
 - związanym z lekceważeniem zasad ochrony danych polegającym na pozostawianiu pomieszczenia lub stanowiska pracy bez ich zabezpieczenia,

- związanym z brakiem świadomości niebezpieczeństwa dopuszczania osób postronnych do swojego stanowiska pracy,
- związanym z atakami z sieci uniemożliwiającymi przetwarzanie (ataki typu DoS na serwer/serwery),
- związanym z działaniami mającymi na celu zaburzenie integralności danych, w celu uniemożliwienia ich przetwarzania lub osiągnięcia korzyści,
- związanym z kradzieżą sprzętu lub nośników z danymi, które zazwyczaj są niezabezpieczone,
- związanym z przekazywaniem sprzętu z danymi do serwisu,
- związanym z kradzieżami tożsamości umożliwiającymi podszywanie się pod inną osobę,
- związanym z podszywaniem się przez osoby nieuprawnione pod witrynę internetową, która zbiera dane,
- i innym zagrożeniom mogącym wystąpić w przyszłości w związku z rozwojem technik i metod przetwarzania danych.

III. Na podstawie 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 (ogólnego rozporządzenia o ochronie) Dz.U. UE.L. 2016.119.1 , ustala się następujące wytyczne polityki bezpieczeństwa danych osobowych przetwarzanych w firmie Emm Consulting

I. POSTANOWIENIA OGÓLNE

Art. 1

1. Dane osobowe w firmie Emm Consulting przetwarzane są z poszanowaniem obowiązujących w tym zakresie przepisów prawa, a w szczególności:
 - a) na podstawie 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 (ogólnego rozporządzenia o ochronie) Dz.U. UE.L. 2016.119.1
 - b) przepisów art.221 §1 - 5 ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (tekst jednolity z 1998 r.: Dz.U.Nr21, poz.94 z późniejszymi zmianami) i przepisów wykonawczych z nią związanych,
 - c) oraz innych przepisów ustaw i rozporządzeń normujących przetwarzanie danych osobowych określonych kategorii.

Art. 2

Polityka bezpieczeństwa w zakresie ochrony danych osobowych w firmie Emm Consulting odnosi się do danych osobowych przetwarzanych w zbiorach danych:

1. **tradycyjnych, w szczególności w kartotekach, skorowidzach, księgach, wykazach i w innych zbiorach ewidencyjnych,**
2. **w systemach informatycznych, także w przypadku przetwarzania danych poza zbiorem danych osobowych.**

Art. 3

1. Emm Consulting realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych dokłada szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności zapewnia, aby dane te były:
 - a) przetwarzane zgodnie z prawem,
 - b) zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami,
 - c) merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane,
 - d) przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

Art. 4

1. Emm Consulting realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych stosuje odpowiednie środki informatyczne, techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności:
 - a) zabezpiecza dane przed ich udostępnieniem osobom nieupoważnionym,
 - b) zabranianiem przez osobę nieuprawnioną,
 - c) przetwarzaniem z naruszeniem ustawy,
 - d) zmianą, utratą, uszkodzeniem lub zniszczeniem.
2. Emm Consulting realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych dąży do systematycznego unowocześniania stosowanych na jego terenie informatycznych, technicznych i organizacyjnych środków ochrony tych danych.
3. W szczególności Emm Consulting zapewnia aktualizacje informatycznych środków ochrony danych osobowych pozwalającą na zabezpieczenie przed wirusami, nieuprawnionym dostępem oraz inni zagrożeniami danych, płynącymi z funkcjonowania systemu informatycznego oraz sieci telekomunikacyjnych.

Art. 5

1. Emm Consulting realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych sprawuje kontrolę i nadzór nad niszczeniem zbędnych danych osobowych i/lub ich zbiorów.
2. Niszczenie zbędnych danych osobowych i/lub ich zbiorów polegać powinno w szczególności na:
 - a) Trwałym, fizycznym zniszczeniu danych osobowych i/lub ich zbiorów wraz z ich nośnikami w stopniu uniemożliwiającym ich późniejsze odtworzenie przez osoby niepowołane przy zastosowaniu powszechnie dostępnych metod.
 - b) **Anonimizacji** danych osobowych i/lub ich zbiorów polegającej na pozbawieniu danych osobowych i/lub ich zbiorów cech pozwalających na identyfikację osób fizycznych, których anonimizowane dane dotyczą.
3. Osoby przetwarzające dane osobowe w firmie Emm Consulting mają obowiązek stosowania oddanych im do dyspozycji narzędzi i technik niszczenia zbędnych danych osobowych i/lub ich zbiorów.
4. **Naruszanie przez zatrudnione osoby i osoby upoważnione do dostępu i/lub przetwarzania danych osobowych stosowanych w firmie Emm Consulting procedur niszczenia zbędnych danych osobowych i/lub ich zbiorów traktowane będzie, jako ciężkie naruszenie podstawowych obowiązków z wszystkimi**

wynikającym stąd konsekwencjami m.in. z rozwiązaniem stosunku pracy włącznie.

5. Kontrola i nadzór nad niszczeniem zbędnych danych osobowych i/lub ich zbiorów może w szczególności polegać na wprowadzeniu odpowiednich procedur niszczenia danych, także zleceniu niszczenia ich, wyspecjalizowanym podmiotom zewnętrznym, gwarantującym bezpieczeństwo procesu niszczenia danych odpowiednie do rodzaju nośnika tych danych.

II. UDOSTĘPNIANIE DANYCH OSOBOWYCH

Art. 6

1. Emm Consulting realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych udostępnia przetwarzane na jego obszarze dane osobowe wyłącznie osobom do tego upoważnionym na mocy uregulowań wewnętrznych obowiązujących w tym zakresie na jego obszarze.
2. Upoważnienie, o którym mowa w art. 7 pkt1, wynikać może w szczególności:
 - a) z charakteru pracy wykonywanej na danym stanowisku pracy, lub
 - b) z dokumentu określającego zakres obowiązków (zakres czynności) wykonywanych na danym stanowisku pracy, lub
 - c) z odrębnego dokumentu zawierającego imienne upoważnienie do dostępu do danych osobowych.

Art. 7

1. Emm Consulting realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych zapewnia dostęp do przetwarzanych danych osobowych osobom fizycznym będącym dysponentami tych danych.
2. Dysponentami danych osobowych są osoby, które powierzyły swoje dane Emm Consulting w związku z realizacją projektów, w tym w szczególności projektów finansowanych ze środków Europejskiego Funduszu Społecznego.

Art. 8

1. Dostęp do danych osobowych i ich przetwarzanie bez odrębnego upoważnienia administratora danych osobowych lub upoważnionej przezeń osoby może mieć miejsce wyłącznie w przypadku działań podmiotów upoważnionych na mocy odpowiednich przepisów prawa do dostępu i przetwarzania danych określonej kategorii.
2. W szczególności dostęp do danych osobowych na wskazanej w art. 10 ust. 1 zasadzie mogą mieć: Państwowa Inspekcja Pracy, Zakład Ubezpieczeń Społecznych, organy skarbowe, Policja, Agencja Bezpieczeństwa Wewnętrznego, Wojskowe Służby Informacyjne, sady powszechne, Najwyższa Izba Kontroli, Generalny Inspektor Ochrony Danych Osobowych inne upoważnione przez przepisy prawa podmioty i organy, działające w granicach przyznanych im uprawnień - wszystkie ww. po okazaniu dokumentów potwierdzających te uprawnienia.

III. OSOBY PRZETWARZAJĄCE DANE OSOBOWE

Art. 9

1. Emm Consulting realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych wyznacza osoby odpowiedzialne za bieżącą realizację tej polityki na terenie firmy. W szczególności wyznaczeni zostają:
 - a) administrator danych osobowych,
 - b) osoby odpowiedzialne za nadzór nad przestrzeganiem zasad ochrony danych osobowych wynikającym z przepisów prawa oraz uregulowań wewnętrznych,
 - c) administrator bezpieczeństwa informacji,
 - d) inne osoby wykonujące zadania ochrony danych osobowych.
2. Wyżej wymienieni wyznaczeni zostają przez właściciela firmy.

Art. 10

1. Emm Consulting realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych dopuszcza do ich przetwarzania w systemie informatycznym i/lub tradycyjnym wyłącznie osoby posiadające upoważnienie nadane przez administratora danych osobowych lub inną upoważnioną do tego osobę.
2. Upoważnienie, o którym mowa w art. 12 pkt1, wynikać może w szczególności:
 - a) z charakteru pracy wykonywanej na danym stanowisku pracy lub
 - b) z dokumentu określającego zakres obowiązków (zakres czynności) wykonywanych na danym stanowisku pracy, lub
 - c) z odrębnego dokumentu zawierającego imienne upoważnienie do dostępu do danych osobowych.

Art. 11

Emm Consulting realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych zapewnia kontrolę nad dostępem do tych danych. Kontrola ta w szczególności realizowana jest poprzez ewidencjonowanie osób przetwarzających dane osobowe oraz wdrożenie procedur udzielania dostępu do tych danych.

Art. 12

1. Emm Consulting realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych zapewnia zaznajomienie osób upoważnionych do dostępu i/lub przetwarzania danych osobowych z powszechnie obowiązującymi przepisami prawa, uregulowaniami wewnętrznymi, a także technikami i środkami ochrony tych danych.
2. W szczególności osoby, wskazane w art. 14 ust. 1, zaznajamiane są z kwestiami wymienionymi w tym przepisie przed dopuszczeniem do pracy na stanowiskach związanych z przetwarzaniem danych osobowych, a także odpowiednio, w trakcie trwania zatrudnienia - w przypadku zmian w obowiązujących przepisach prawa, uregulowaniach wewnętrznych lub technikach i środkach ochrony danych stosowanych w firmie Emm Consulting.
3. Zaznajomienie osób upoważnionych do przetwarzania danych osobowych z powszechnie obowiązującymi przepisami prawa, uregulowaniami wewnętrznymi, a także technikami i środkami ochrony tych danych stosowanymi w firmie Emm Consulting może odbywać się w szczególności poprzez:
 - a. instruktaż na stanowisku pracy,
 - b. szkolenie wewnętrzne

- c. szkolenie zewnętrzne.

Art. 13

Osoby upoważnione przez Emm Consulting do przetwarzania danych osobowych zostają zaznajomione z zakresem informacji objętych tajemnicą w związku z wykonywaną przez siebie pracą. W szczególności są one informowane o powinności zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia stosowanych w Emm Consulting.

Art. 14

Naruszanie przez osoby zatrudnione w ramach stosunku pracy, oraz osoby upoważnione do dostępu i/lub przetwarzania danych osobowych, zasad bezpiecznego i zgodnego z prawem ich przetwarzania, traktowane będzie jako ciężkie naruszenie podstawowych obowiązków.

IV. PRAWA OSÓB , KTÓRYCH DANE SĄ PRZETWARZANE PRZEZ Emm Consulting

Art. 15

1. W szczególności każdej osobie fizycznej, której dane osobowe są przetwarzane, przysługuje prawo do uzyskania informacji o zakresie jej uprawnień związanych z ochroną danych osobowych, a także prawo do kontroli przetwarzania danych, które jej dotyczą,
2. Osoby fizyczne, których dane osobowe są przetwarzane, uzyskują informacje o przysługujących im prawach w sposób przyjęty przez Emm Consulting.

V. BUDYNKI, POMIESZCZENIA I CZĘŚCI POMIESZCZEŃ, W KTÓRYCH PRZETWARZANE SĄ DANE OSOBOWE

Art. 16

1. Emm Consulting realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych wyznacza budynki, pomieszczenia i części pomieszczeń, w którym przetwarzane są dane osobowe.
2. **W przypadku, gdy w pomieszczeniu znajduje się część ogólnodostępna oraz część, w której przetwarzane są dane osobowe – część, w której są przetwarzane dane osobowe powinna być wyraźnie oddzielona od ogólnodostępnej.**
3. Wydzielenie części pomieszczenia, w której przetwarza się dane osobowe może być w szczególności dokonane poprzez montaż barierki, lad lub odpowiednie ustawienie mebli biurowych uniemożliwiający lub co najmniej ograniczający niekontrolowany dostęp osób niepowołanych do zbiorów danych osobowych przetwarzanych w danym pomieszczeniu.
4. **Pod szczególną ochroną przed niepowołanym dostępem do danych osobowych pozostają urządzenia wchodzące w skład systemu informatycznego**

Emm Consulting. W szczególności stacje robocze (poszczególne komputery) wchodzące w skład tego systemu, powinny być umiejscawiane w sposób uniemożliwiający osobom nieuprawnionym, bezpośredni i niekontrolowany dostęp do ekranów oraz urządzeń służących do przetwarzania, a zwłaszcza kopiowania danych.

Art. 17

1. Całkowite opuszczenie pomieszczenia, w którym przetwarzane są dane osobowe, musi
2. wiązać się z zastosowaniem dostępnych środków zabezpieczających to pomieszczenie przed wejściem osób niepowołanych.
3. Opuszczenie pomieszczenia, w którym przetwarzane są dane osobowe, musi wiązać się z zastosowaniem dostępnych środków zabezpieczających używane aktualnie zbiory danych osobowych. W szczególności w razie planowanej, choćby chwilowej, nieobecności
4. pracownika upoważnionego do przetwarzania danych osobowych obowiązany jest on umieścić zbiory występujące w formach tradycyjnych w odpowiednio zabezpieczonym miejscu ich przechowywania oraz dokonać niezbędnych operacji w systemie informatycznym uniemożliwiającym dostęp do danych osobowych osobom niepowołanym.
5. Opuszczenie przez pracownika przetwarzającego dane osobowe obszaru ich przetwarzania bez zabezpieczenia budynku i/lub pomieszczenia oraz umiejscowionych w nim zbiorów danych jest niedopuszczalne, i jako takie traktowane będzie, jako ciężkie naruszenie podstawowych obowiązków pracowniczych.

VI. REGULACJE ZWIĄZANE Z WIZERUNKIEM UCZESTNIKÓW USŁUGI ROZWOJOWEJ

1. Uczestnik usługi rozwojowej wyraża zgodę na fotografowanie i nagrywanie przebiegu usługi rozwojowej, późniejszą publikację zdjęć, nagrań audio/video ze szkoleń oraz na użycie ich wizerunku, podobieństwa, głosu. Uczestnicy oświadczają, że nie będą mieli jakichkolwiek roszczeń z tym związanych pod warunkiem, że zdjęcia, nagrania audio/video oraz inne materiały zawierające wizerunek podobieństwo Uczestnika szkolenia będą wykorzystywane jedynie w celu związanym z rozliczeniem projektów ze wsparciem środków publicznych. Osoba, która takiej zgody nie wyrazi zobowiązana jest do poinformowania środkami komunikacji elektronicznej o rezygnacji najpóźniej drugiego dnia po zakończeniu usługi rozwojowej.
2. Organizator nie ponosi odpowiedzialności za wykorzystanie wizerunku Uczestnika przez innego Uczestnika usługi rozwojowej bądź Klienta.