POLITYKA OCHRONY DANYCH [POLITYKA BEZPIECZEŃSTWA INFORMACJI]

W

.....
.....
[nazwa firmy]

.....
[data sporządzenia]

§1
CEL POWSTANIA DOKUMENTU I OŚWIADCZENIA ADMINISTRATORA DANYCH OSOBOWYCH

1. Niniejsza *Polityka ochrony danych,* zwana dalej *Polityką* lub *Polityką bezpieczeństwa*, została sporządzona i wdrożona w celu wykazania, że dane osobowe są przetwarzane i zabezpieczone zgodnie z wymogami prawa, dotyczącymi zasad przetwarzania i zabezpieczenia danych w firmie, w tym z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 (dalej jako RODO).
2. Przedmiotem Polityki jest m.in. określenie, opisanie i zawarcie w niej, jak również w załączonych dokumentach:
   a) zasad przetwarzania danych osobowych,
   b) zastosowanych środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń,
   c) kategorii danych osobowych objętych ochroną, a w szczególności:
      - zabezpieczeń danych osobowych przed ich udostępnieniem osobom nieupoważnionym,
      - zabraniem przez osobę nieuprawnioną,
      - przetwarzaniem z naruszeniem ustawy,
      - zmianą, utratą, uszkodzeniem lub zniszczeniem.

3. …….. [nazwa firmy] jest Administratorem Danych Osobowych osób fizycznych, które są przetwarzane w ramach prowadzonej przez niego działalności gospodarczej.
4. Administrator zapewnia, że:
   a) nie prowadzi przetwarzania danych, które wiązałoby się z wysokim ryzykiem naruszenia praw lub wolności osoby fizycznej;
   b) uwzględnia ochronę danych w fazie projektowania oraz stosuje domyślną politykę ochrony tam, gdzie ma to zastosowanie (tzw. *„privacy by design" i „privacy by default"*);
   c) respektuje prawa osoby, której dane dotyczą, w szczególności prawa dostępu do danych, sprostowania danych, bycia zapomnianym, prawo do ograniczenia przetwarzania, prawo do przenoszenia danych, prawo do sprzeciwu, zgodnie z aktualnie obowiązującymi przepisami prawa;

   d) dokona oceny skutków dla planowanych operacji przetwarzania danych osobowych przed rozpoczęciem przetwarzania - jeśli dany rodzaj przetwarzania - w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych.

5. Administrator Danych Osobowych nie podlega obowiązkowi powołania Inspektora Ochrony Danych Osobowych. Samodzielnie wykonuje jego zadania, zgodnie z aktualnie obowiązującymi przepisami prawa.
6. Pracownicy i współpracownicy Administratora Ochrony Danych Osobowych są zobowiązani do zapoznania się z obowiązującymi procedurami i instrukcjami, a także postępowania zgodnie z nimi.

§2
DEFINICJE

1. **Administrator Danych Osobowych lub Administrator -** . . . .……………………………... . . . . [nazwa firmy – imię, nazwisko, firma, adres]
2. **Dane osobowe zwykłe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. 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, np.: imię, nazwisko, numer PESEL, adres e-mail, data urodzenia, adres zamieszkania.
3. **Dane osobowe wrażliwe** – dane osobowe, ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, stan zdrowia i wszelkie informacje dotyczące zdrowia psychicznego lub fizycznego, kod genetyczny, dane genetyczne i biometryczne, nałogi lub życie seksualne, dotyczące skazań, orzeczeń o ukaraniu, mandatów karnych.
4. **System informatyczny** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji narzędzi programowych zastosowanych w celu przetwarzania danych.
5. **Użytkownik** – osoba upoważniona przez Administratora Danych do Przetwarzania danych osobowych. Użytkownikiem może być pracownik, osoba wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilnoprawnej.

6. **Identyfikator użytkownika** – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym (Użytkownika) w razie Przetwarzania danych osobowych w takim systemie.
7. **Odbiorca danych –** każdy, komu udostępnia się dane osobowe, z wyłączeniem:
   - Osoby, której dane dotyczą,
   - Osoby upoważnionej do przetwarzania danych,
   - Podmiotu, któremu powierzono przetwarzanie danych,
   - Organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.
8. **Osoba upoważniona –** osoba, która została upoważniona przez Administratora danych osobowych do przetwarzania danych w celu i w zakresie wskazanym w upoważnieniu. Może nią być osoba zatrudniona na podstawie umowy o pracę, umowy cywilnoprawnej, wolontariusz, stażysta, itp.
9. **Zbiór danych** – każdy uporządkowany zestaw danych o charakterze osobowym, dostępny według określonych kryteriów, niezależnie od tego czy jest rozproszony, czy podzielony funkcjonalnie.
10. **Przetwarzanie danych** – jakiekolwiek operacje wykonywane na Danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie w formie tradycyjnej oraz w systemach informatycznych. Zasady zawarte w niniejszej Polityce należy stosować przy każdej operacji na danych.
11. **Udostępnienie danych** – przekazanie danych osobowych innemu administratorowi danych na podstawie właściwych przepisów prawa, np. sądowi, policji, prokuraturze.
12. **Powierzenie danych –** przekazanie danych osobowych innemu podmiotowi w określonym celu i zakresie, na podstawie zawartej umowy i w ramach jej realizacji, np. umowy z biurem rachunkowym.
13. **Hasło** – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym (Użytkownikowi) w razie przetwarzania danych osobowych w takim systemie.
14. **Uwierzytelnianie** – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu (Użytkownika) w systemach informatycznych, najczęściej polegające na wpisaniu loginu i hasła użytkownika.
15. **RODO** – oznacza Rozporządzenie Parlamentu Europejskiego i Rady EU 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).

§3

POSTANOWIENIA OGÓLNE I OBOWIĄZKI ADMINISTRATORA

1. Polityka dotyczy wszystkich danych osobowych przetwarzanych w . . . . . [nazwa firmy], niezależnie od formy ich przetwarzania (przetwarzane tradycyjnie zbiory ewidencyjne, systemy informatyczne) oraz od tego, czy dane są lub mogą być przetwarzane w zbiorach danych.
2. Polityka jest przechowywana w wersji elektronicznej oraz w wersji papierowej w siedzibie Administratora.
3. Polityka jest udostępniana do wglądu osobom posiadającym upoważnienie do przetwarzania danych osobowych na ich wniosek, a także osobom, którym ma zostać nadane upoważnienie do przetwarzania danych osobowych, celem zapoznania się z jej treścią.
4. Dokument Polityki, wraz z załącznikami, stanowi tajemnicę przedsiębiorstwa Administratora Danych Osobowych i jest klasyfikowany jako dokument wewnętrzny.
5. Dla skutecznej realizacji Polityki Administrator Danych zapewnia:
   a) odpowiednie do zagrożeń i kategorii danych objętych ochroną środki techniczne i rozwiązania organizacyjne,
   b) kontrolę i nadzór nad Przetwarzaniem danych osobowych,
   c) monitorowanie zastosowanych środków ochrony.
6. Monitorowanie przez Administratora Danych zastosowanych środków ochrony obejmuje m.in. działania Użytkowników, naruszanie zasad dostępu do danych, zapewnienie integralności plików oraz ochronę przed atakami zewnętrznymi oraz wewnętrznymi.
7. Administrator Danych zapewnia, że czynności wykonywane w związku z przetwarzaniem i zabezpieczeniem danych osobowych są zgodne z niniejszą polityką oraz odpowiednimi przepisami prawa.
8. Polityka obejmuje:
   1) wszystkie zbiory danych osobowych przetwarzane przez Administratora (w formie elektronicznej i papierowej) oraz dane przetwarzane poza zbiorami danych,
   2) wszystkich pracowników oraz osoby, przy pomocy których Administrator wykonuje swoje czynności, mające dostęp do danych osobowych, przy czym za pracownika uważa się osobę zatrudnioną na podstawie umowy o pracę, powołania, wyboru, mianowania, umowy cywilnoprawnej, a także inną osobę współpracującą z pracodawcą, m.in. wolontariusza czy osobę fizyczną prowadzącą działalność gospodarczą.
9. Każde naruszenie zasad Polityki może być uznane za poważne naruszenie podstawowych obowiązków pracowniczych lub wynikających z umów cywilnoprawnych o współpracy, i może skutkować konsekwencjami i odpowiedzialnością przewidzianymi w przepisach

prawnych, takich jak m.in. ustawa Kodeks pracy, ustawa Kodeks cywilny, czy ustawa o ochronie danych osobowych i RODO.

§4

DANE OSOBOWE PRZETWARZANE U ADMINISTRATORA DANYCH

1. Dane osobowe przetwarzane przez Administratora Danych gromadzone są w zbiorach danych oraz poza zbiorami, w wersji papierowej oraz elektronicznej.
2. Administrator prowadzi opis zbiorów danych osobowych jak wskazano w Rejestrze czynności przetwarzania danych. Zawiera on m.in. czynności przetwarzania oraz kategorie danych.
3. Administrator danych nie podejmuje czynności przetwarzania, które mogłyby się wiązać z poważnym prawdopodobieństwem wystąpienia wysokiego ryzyka dla praw i wolności osób. W przypadku planowania takiego działania Administrator wykona czynności określone w art. 35 i nast. RODO (dokona analizy skutków dla ochrony danych).
4. W przypadku planowania nowych czynności przetwarzania Administrator, jeśli uzna to za konieczne, dokona analizy ich skutków dla ochrony danych osobowych oraz uwzględni kwestie ochrony danych w fazie ich projektowania.

ZAŁĄCZNIK: Identyfikacja danych osobowych u Administratora

ZAŁĄCZNIK: Analiza ryzyka

§5

REJESTR CZYNNOŚCI PRZETWARZANIA

1. Administrator dokonuje inwentaryzacji danych w ramach **Rejestru Czynności Przetwarzania Danych,** zwanego dalej Rejestrem.
2. Rejestr stanowi formę dokumentowania czynności przetwarzania danych, pełni rolę mapy przetwarzania danych i jest jednym z kluczowych elementów umożliwiających realizację fundamentalnej zasady, na której opiera się cały system ochrony danych osobowych, czyli zasady rozliczalności.
3. Rejestr powinien być systematycznie prowadzony i aktualizowany (o ile zachodzi taka potrzeba).
4. W przypadku gdy Administrator w relacjach z innymi podmiotami jest podmiotem przetwarzającym, Administrator prowadzi także **Rejestr kategorii przetwarzania**.

ZAŁĄCZNIK: Rejestr czynności przetwarzania

ZAŁĄCZNIK: Rejestr kategorii czynności przetwarzania (jeśli dotyczy)

§6
PODSTAWOWE ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

1. Administrator przetwarza dane osobowe wyłącznie, gdy jest to dopuszczone aktualnie obowiązującymi przepisami prawa.
2. Dane osobowe mogą być przetwarzane wyłącznie w celu i zakresie, w jakim zostały zgromadzone, a także nie dłużej niż jest to niezbędne dla osiągnięcia tego celu.
3. Dane osobowe po wykorzystaniu są niezwłocznie usuwane lub przechowywane wyłącznie w postaci uniemożliwiającej identyfikację osób, których dotyczą, o ile przepisy odrębnych ustaw nie podają określonego czasu przechowywania danych.
4. Dane osobowe są przetwarzane przez Administratora, gdy:
   a) osoba, której dane dotyczą wyraziła na to zgodę, np. newsletter;
   b) jest to niezbędne do wykonania umowy, której strona jest osobą lub do podjęcia działań na żądanie osoby, której dane dotyczą przed zawarciem umowy, np. e-sklep, zawarcie umowy na wykonanie usługi;
   c) jest to niezbędne do wypełnienia obowiązku prawnego ciążącego na Administratorze Danych Osobowych, np. w związku z zatrudnieniem;
   d) jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora lub przez podmiot trzeci, np. marketing własnych produktów lub usług;
   e) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, np. ochrona zdrowia lub życia.

5. Administrator Danych przetwarza szczególne kategorie danych, **tzw. dane wrażliwe**, gdy:
   a) jest to niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez Administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone przepisami prawa,
   b) osoba, której dane dotyczą wyraziła na to zgodę,
   c) jest to niezbędne do ustalenia, dochodzenia lub obrony roszczeń, związanych z udzielonymi usługami w ramach wykonywanej przez Administratora działalności gospodarczej.
7. W przypadku gdy dane osobowe są niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy lub są zbędne do realizacji celu, dla którego zostały

zebrane, Administrator jest zobowiązany do ich uzupełnienia, uaktualnienia, sprostowania lub usunięcia.

8. Administrator stosuje ogólne zasady przetwarzania danych osobowych zawarte w RODO, w szczególności w art. 5 RODO.

ZAŁĄCZNIK: Obowiązek informacyjny – wzory niezbędnych klauzul informacyjnych

ZOBACZ: Obowiązek informacyjny – w przypadku rekrutacji pracowników wraz z ich zgodą – wzór (jeśli dotyczy)

§7
OBOWIĄZKI I ODPOWIEDZIALNOŚĆ W ZAKRESIE ZARZĄDZANIA BEZPIECZEŃSTWEM DANYCH

1. Wszystkie osoby zobowiązane są do przetwarzania danych osobowych zgodnie z obowiązującymi przepisami i zgodnie z ustaloną przez Administratora Danych Polityką Bezpieczeństwa (Polityką Ochrony Danych), Instrukcją Zarządzania Systemem Informatycznym, a także innymi dokumentami wewnętrznymi i procedurami związanymi z przetwarzaniem danych osobowych w . . . . . [nazwa firmy].
2. Wszystkie dane osobowe u Administratora są przetwarzane z poszanowaniem zasad przetwarzania przewidzianych przez przepisy prawa:
   a) w każdym wypadku występuje chociaż jedna z przewidzianych przepisami prawa podstaw dla przetwarzania danych,
   b) dane przetwarzane są rzetelnie i w sposób przejrzysty,
   c) dane osobowe zbierane są w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami,
   d) dane osobowe są przetwarzane jedynie w takim zakresie, jaki jest niezbędny dla osiągnięcia celu przetwarzania danych,
   e) dane osobowe są prawidłowe i w razie potrzeby uaktualniane,
   f) czas przechowywania danych jest ograniczony do okresu ich przydatności do celów, do których zostały zebrane, a po tym okresie są one anonimizowane bądź usuwane,
   g) wobec osoby, której dane dotyczą, wykonywany jest obowiązek informacyjny zgodnie z treścią art. 13 i 14 RODO,
   h) dane są zabezpieczone przed naruszeniami zasad ich ochrony.

3. Za naruszenie lub próbę naruszenia zasad przetwarzania i ochrony Danych osobowych uważa się w szczególności:
   a) naruszenie bezpieczeństwa Systemów informatycznych, w których przetwarzane są dane osobowe, w razie ich przetwarzania w takich systemach;
   b) udostępnianie lub umożliwienie udostępniania danych osobom lub podmiotom do tego nieupoważnionym;
   c) zaniechanie, choćby nieumyślne, dopełnienia obowiązku zapewnienia danym osobowym ochrony;
   d) niedopełnienie obowiązku zachowania w tajemnicy Danych osobowych oraz sposobów ich zabezpieczenia;
   e) przetwarzanie Danych osobowych niezgodnie z założonym zakresem i celem ich zbierania;
   f) spowodowanie uszkodzenia, utraty, niekontrolowanej zmiany lub nieuprawnione kopiowanie Danych osobowych;
   g) naruszenie praw osób, których dane są przetwarzane.
4. W przypadku stwierdzenia okoliczności naruszenia zasad ochrony danych osobowych Użytkownik zobowiązany jest do podjęcia wszystkich niezbędnych kroków, mających na celu ograniczenie skutków naruszenia i do niezwłocznego powiadomienia Administratora Danych.
5. Do obowiązków Administratora Danych w zakresie zatrudniania, zakończenia lub zmiany warunków zatrudnienia pracowników lub współpracowników (osób podejmujących czynności na rzecz Administratora Danych na podstawie innych umów cywilnoprawnych) należy dopilnowanie, aby:
   a) pracownicy byli odpowiednio przygotowani do wykonywania swoich obowiązków,
   b) każdy z przetwarzających Dane osobowe był pisemnie upoważniony do przetwarzania danych zgodnie z „Upoważnieniem do przetwarzania danych osobowych”
   c) każdy pracownik lub współpracownik zobowiązał się do zachowania danych osobowych przetwarzanych u Administratora w tajemnicy poprzez podpisanie „Oświadczenia o poufności”.
6. Pracownicy i współpracownicy zobowiązani są do:
   a) ścisłego przestrzegania zakresu nadanego upoważnienia;
   b) przetwarzania i ochrony danych osobowych zgodnie z przepisami;
   c) zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia;
   d) zgłaszania incydentów związanych z naruszeniem bezpieczeństwa danych oraz niewłaściwym funkcjonowaniem systemu.
7. Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby, które posiadają imienne upoważnienie nadane przez Administratora Danych Osobowych.

§8
OBOWIĄZKI OSÓB UPOWAŻNIONYCH

1. Dane osobowe mogą być przetwarzane wyłącznie w oparciu o upoważnienie do przetwarzania. Nadane upoważnienia obejmuje także nadanie odpowiednich uprawnień do systemu przetwarzającego dane osobowe.
2. Każdy pracownik, który nie ma dostępu do danych osobowych i nie posiada upoważnienia, powinien zostać zobowiązany do zachowania danych osobowych przetwarzanych u Administratora w tajemnicy poprzez podpisanie „Oświadczenia o poufności".
3. Osoba upoważniona podpisuje oświadczenie zawierające zobowiązania do przetwarzania danych zgodnie z RODO.
4. Upoważnienie wydawane jest przed rozpoczęciem przetwarzania danych osobowych na czas trwania umowy o pracę lub innej umowy cywilnoprawnej, a także na czas wykonania określonego zadania, które związane jest z przetwarzaniem danych, w celu i zakresie wynikającym z zadań i obowiązków służbowych.
5. Każda osoba, która uzyskała upoważnienie do przetwarzania danych osobowych zobowiązana jest do:
   1) przetwarzania ich co do zasady wyłącznie na polecenia Administratora,
   2) ochrony danych w sposób zgodny z przepisami prawa i wewnętrznymi zaleceniami,
   3) zachowania w tajemnicy danych osobowych i sposobów ich zabezpieczania.

   Osoba upoważniona składa oświadczenie o przetwarzaniu danych w tym zakresie zgodnie z załącznikiem do Polityki.

6. Osoba upoważniona do przetwarzania danych jest zobowiązana do:

a) przetwarzania danych osobowych zgodnie z upoważnieniem wydanym przez Administratora Danych Osobowych;
b) stosowania się do instrukcji i procedur przetwarzania danych osobowych, zawartych w politykach wewnętrznych wydanych przez Administratora Danych Osobowych;
c) stosowania wprowadzonych środków organizacyjnych i technicznych, zapewniających ochronę przetwarzania danych, w szczególności przed ich udostępnieniem, kradzieżą, uszkodzeniem lub zniszczeniem przez osoby nieupoważnione;
d) umożliwienia przeprowadzenia czynności w toku sprawdzenia planowanego lub doraźnego prowadzonego przez Administratora Danych Osobowych lub na jego zlecenie;

e) sprawowania nadzoru nad obiegiem oraz przechowywaniem i zabezpieczeniem dokumentów zawierających dane osobowe, do których ma dostęp w chwili wykonywania czynności służbowych;
f) każdorazowego niezwłocznego informowania Administratora Danych Osobowych w sytuacji naruszenia ochrony danych osobowych lub uzasadnionego podejrzenia takiego naruszenia.

7. Podczas przetwarzania danych trzeba zachować szczególną ostrożność i podjąć wszelkie możliwe środki umożliwiające zabezpieczenie oraz ochronę danych przed nieuprawnionym dostępem, modyfikacją, utratą, zniszczeniem lub ujawnieniem.
8. Przed nadaniem upoważnienia Administrator lub inna wyznaczona osoba zapoznaje osobę upoważnianą z zasadami i przepisami dot. ochrony danych osobowych,
9. Upoważnienie do przetwarzania danych osobowych powinno zawierać:
   1) datę z którą zostało nadane;
   2) datę, z którą upoważnienie wygasa jeżeli jest ono nadane na czas określony;
   3) zakres upoważnienia.
10. Upoważnienie do przetwarzania danych osobowych wygasa z chwilą upływu terminu wypowiedzenia lub rozwiązania umowy zawartej przez Administratora z osobą, której zostało nadane lub w przypadku, gdy zostało nadane na czas określony z upływem czasu na jaki zostało nadane bądź w z chwilą cofnięcia upoważnienia.
11. Zakres nadanych upoważnień może też ulegać zmianie (rozszerzeniu bądź zawężeniu) w związku z pełnieniem przez osobę określonych zadań w określonym czasie. W przypadku ustania podstaw do przetwarzania danych osobowych, Administrator Danych Osobowych uchyla upoważnienie do przetwarzania danych osobowych.
12. Prowadzi się rejestr osób upoważnionych do przetwarzania danych. Przykładowy wzór rejestru osób upoważnionych stanowi załącznik do Polityki.
13. Rejestr ten powinien umożliwić ustalenie kolejności nadawanych uprawnień danej osobie (np. numer porządkowy), co umożliwi zachowanie zasad rozliczalności w przetwarzaniu danych osobowych.
14. Administrator Danych Osobowych aktualizuje rejestr osób upoważnionych za każdym razem, gdy upoważnia do przetwarzania nowe osoby, zmienia zakres i cel nadanego już upoważnienia lub, gdy osoba upoważniona zakończy z nim współpracę.

ZAŁĄCZNIK: Upoważnienie do przetwarzania danych osobowych (jeśli dotyczy)
ZAŁĄCZNIK: Oświadczenie o poufności (jeśli dotyczy)
ZAŁĄCZNIK: Rejestr osób upoważnionych do przetwarzania danych osobowych (jeśli dotyczy)

OBOWIĄZEK INFORMACYJNY REALIZOWANY PRZEZ ADMINISTRATORA

1. Administrator Danych Osobowych respektuje prawa, które przysługują każdej osobie, której dane dotyczą, w szczególności prawo do kontroli przetwarzania danych.
2. Administrator Danych informuje osoby, których dane dotyczą, o swoich danych, adresie, siedzibie, celu zbierania danych, obowiązku lub dobrowolności ich podania, a także przekazuje inne informacje, które mogą być wymagane aktualnie obowiązującymi przepisami prawa.
3. Obowiązek informacyjny w przypadku pozyskiwania danych bezpośrednio od osoby, której dane dotyczą wykonywany jest przed rozpoczęciem ich gromadzenia.
4. Osobę, której dane dotyczą informuje się o:
   a) dokładnej nazwie i adresie swojej siedziby;
   b) celu zbierania danych;
   c) dobrowolności lub obowiązku podania danych, a jeżeli taki obowiązek istnieje o jego podstawie prawnej;
   d) prawie wglądu do treści swoich danych oraz możliwości ich poprawiania;
   e) innych informacjach, wynikających z aktualnych przepisów prawa, w szczególności o:
      - celu przetwarzania danych na podstawie interesu prawnego administratora danych,
      - zamiarze przekazania danych do państwa trzeciego,
      - okresie przez który dane będą przetwarzane, a gdy nie jest możliwe jego ustalenie to o kryteriach ustalenia tego okresu,
      - prawie do żądania sprostowania, usunięcia lub ograniczenia przetwarzania,
      - prawie do wniesienia sprzeciwu wobec przetwarzania,
      - prawie do przenoszenia danych (jeśli przetwarzanie odbywa się na podstawie umowy lub zgody),
      - prawie do cofnięcia zgody w dowolnym momencie (jeśli przetwarzanie odbywa się na podstawie zgody osoby), bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem,
      - prawie wniesienia skargi do organu nadzorczego,
      - profilowaniu i jego konsekwencjach, jeśli jest to zasadne.
5. Powyższych informacji nie udziela się jeśli osoba dysponuje już tymi informacjami, a Administrator będzie w stanie to wykazać lub, gdy obowiązek ich ujawnienia wynika z prawa UE lub prawa krajowego.

6. W przypadku zbierania danych osobowych nie bezpośrednio od osoby, której one dotyczą, osobę tę należy w rozsądnym terminie po pozyskaniu danych osobowych - najpóźniej w ciągu miesiąca - mając na uwadze konkretne okoliczności przetwarzania danych osobowych – poinformować dodatkowo o:
   a) źródle danych;
   b) innych uprawnieniach wynikających z aktualnie obowiązujących przepisów.
7. Administrator ma również na uwadze, że każda osoba, której dane dotyczą, może wystąpić z wnioskiem o otrzymanie informacji o jej danych, które są przetwarzane w zbiorze u Administratora, zgodnie z obowiązującymi przepisami. Odpowiedź na zapytanie osoby, której dane dotyczą, jest udzielana na piśmie w terminie nieprzekraczającym miesiąca od daty wpłynięcia wniosku.
8. Wyłączenie obowiązku udzielenia odpowiedzi następuje wyłącznie w przypadkach, określonych aktualnie obowiązującymi przepisami prawa.
9. Obowiązek informacyjny realizowany jest poprzez podanie niezbędnych informacji na formularzach, umowach, w regulaminie lub kwestionariuszach osobowych.
10. Administrator, głównie celem ochrony **tzw. danych wrażliwych,** jeśli doszłoby do ich przetwarzania, głównie danych o zdrowiu, oraz w celu zapewnienia realizacji praw podmiotów danych, wprowadza i przestrzega u siebie „Procedurę realizacji praw podmiotów danych zgodnie z RODO”.

ZAŁĄCZNIK: Procedura realizacji praw podmiotów danych zgodnie z RODO
ZAŁĄCZNIK: Obowiązek informacyjny – wzory niezbędnych klauzul informacyjnych

§9
UDOSTĘPNIANIE DANYCH OSOBOWYCH

1. Administrator Danych udostępnia dane osobowe przetwarzane w zbiorach danych wyłącznie osobom lub podmiotom uprawnionym do ich otrzymania na podstawie aktualnych przepisów prawnych.
2. Dane osobowe mogą być udostępniane na podstawie:
   a) wniosku od podmiotu uprawnionego do otrzymywania danych osobowych na podstawie przepisów prawa, w szczególności wniosku sądu, prokuratury, policji, komornika, ZUS, Urzędu Skarbowego, itp.,
   b) wniosku innej osoby lub podmiotu, na zasadach określonych w przepisach prawa;

3. Wszystkie osoby upoważnione, które otrzymają wniosek o udostępnienie danych, zobowiązane są do przekazywania go bezpośrednio do Administratora, który podejmuje decyzję o udostępnieniu lub odmowie udostępnienia.
4. Wniosek o udostępnienie danych osobowych powinien zawierać następujące elementy:
   a) Wnioskodawca (Dokładne określenie : nazwa firmy lub jednostki, osoby fizycznej, PESEL, adres siedziby spółki lub adres zamieszkania, NIP, KRS)
   b) Podstawa prawna upoważniająca
   do pozyskania danych albo wskazanie wiarygodnie uzasadnionej potrzeby posiadania danych
   c) Opis lub nazwa zbioru, z którego dane mają być udostępnione
   d) Zakres żądanych danych (np. imię, nazwisko, adres e-mail, adres zamieszkania, itp.)
   e) Informacje umożliwiające wyszukanie w zbiorze danych (np. zapisanie się na newsletter).
5. Zalecane jest prowadzenie **Rejestru udostępnień** według wzoru w załączniku lub w innej formie odnotowywanie sytuacji, w których doszło do udostępnienia danych.

ZAŁĄCZNIK: Procedura realizacji praw podmiotów danych zgodnie z RODO
ZAŁĄCZNIK: Udostępnianie danych - Wykaz udostępnień danych osobom, których te dane dotyczą
ZAŁĄCZNIK: Udostępnianie danych - Wykaz udostępnień danych osobowych innym podmiotom
ZAŁĄCZNIK: Udostępnianie danych - Wniosek o udostępnienie danych osobowych

§10
OBSZAR PRZETWARZANIA DANYCH OSOBOWYCH

1. Obszar, w którym przetwarzane są Dane osobowe na terenie . . . . . [nazwa firmy], obejmuje wszystkie pomieszczenie zlokalizowane w . . . . . [adres firmy].
2. Administrator przetwarza dane jedynie na obszarze do tego przeznaczonym w sposób uniemożliwiający dostęp do danych osobom nieuprawnionym.
3. Obszar przetwarzania danych osobowych jest czasowo lub stale poszerzany w związku z realizacją swoich zadań przez upoważnione podmioty zewnętrzne, tj. podmioty przetwarzające.

4. Obszar przetwarzania danych osobowych może być także czasowo poszerzany o miejsca realizacji konkretnych zleceń – precyzyjne określenie ww. obszarów w niniejszej Polityce nie jest możliwe, ale ze względu na cykliczne pojawianie się takich sytuacji należało sformułować niniejszy zapis.
5. Dodatkowo obszar, w którym przetwarzane są Dane osobowe, stanowią wszystkie komputery przenośne oraz inne nośniki danych (np. pendrive'y, kalendarze, telefony komórkowe, tablety, dyski zewnętrzne) znajdujące się poza obszarem wskazanym powyżej, na których przechowuje się nośniki informacji zawierające dane osobowe.
6. Dostęp do pomieszczenia, w którym dane osobowe są przetwarzane mogą mieć wyłącznie osoby upoważnione. Inne osoby mogą przebywać w obszarze przetwarzania danych wyłącznie pod nadzorem osoby upoważnionej.
7. Gdy nie jest możliwe nadzorowanie pracy osób nieupoważnionych w obszarze przetwarzania danych osobowych, Administrator zapewnia zabezpieczenie danych osobowych, znajdujących się w danym pomieszczeniu, w taki sposób, aby nie było możliwe zabranie, zniszczenie lub jakikolwiek dostęp do tych danych.

ZAŁĄCZNIK: Rejestr pomieszczeń, w którym przetwarzane są dane osobowe (jeśli dotyczy)

§11
SPOSÓB PRZEPŁYWU DANYCH POMIĘDZY SYSTEMAMI

1. Administrator danych nie prowadzi opisu sposobu przepływu danych pomiędzy systemami służącymi do przetwarzania danych osobowych, gdyż dane te przetwarzane są *bez użycia systemu informatycznego / w jednym systemie informatycznym/ w kilku systemach, ale nie zachodzi między nimi przepływ danych.*
2. Administrator danych osobowych prowadzi opis sposobu przepływu danych pomiędzy systemami, służących do przetwarzania danych osobowych i na bieżąco go aktualizuje, jeśli zachodzą jakiekolwiek zmiany.

Oprogramowanie, z którego dane wypływają	Gdzie przepływają dane	Zakres danych

Program księgowy	Serwer dostawcy programu	Np. Imię, nazwisko, adres, PESEL, data urodzenia, numer dowodu osobistego pracowników
Program do wystawiania faktur	Serwer dostawcy programu	Np. Firma, imię, nazwisko, PESEL, NIP – klientów, adres
Program kadrowo - księgowy	Serwer dostawcy programu	Np. Imię, nazwisko, adres, PESEL, data urodzenia, numer dowodu osobistego pracowników
Program do wysyłki newsletterów	Serwer dostawcy newslettera	Np. Imię, nazwisko, data urodzenia, adres e-mail – osób zapisujących się na newsletter
Inne….		
Inne….		

ZAŁĄCZNIK: Instrukcja zarządzania systemem informatycznym

ZAŁĄCZNIK: Wniosek o nadanie dostępu do systemu informatycznego (jeśli dotyczy)

ZAŁĄCZNIK: Rejestr kont, osób i systemów przetwarzających dane (jeśli dotyczy)

§12

OKREŚLENIE ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH NIEZBĘDNYCH DLA ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH

1. Administrator Danych zapewnia zastosowanie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności, rozliczalności i ciągłości Przetwarzanych danych.
2. Zastosowane środki ochrony (techniczne i organizacyjne) powinny być adekwatne do stwierdzonego poziomu ryzyka dla poszczególnych systemów, rodzajów zbiorów i kategorii danych. Środki obejmują w szczególności:

a) Ograniczenie dostępu do pomieszczeń, w których przetwarzane są dane osobowe, jedynie do osób odpowiednio upoważnionych. Inne osoby mogą przebywać w pomieszczeniach wykorzystywanych do przetwarzania danych jedynie w towarzystwie osoby upoważnionej.
b) Zamykanie pomieszczeń tworzących obszar Przetwarzania danych osobowych określony w §10 na czas nieobecności pracowników/współpracowników, w sposób uniemożliwiający dostęp do nich osobom trzecim.
b) Wykorzystanie zamykanych szafek i/lub sejfów do zabezpieczenia dokumentów.
c) Wykorzystanie niszczarki do skutecznego usuwania dokumentów zawierających dane osobowe.
d) Ochronę sieci lokalnej przed działaniami inicjowanymi z zewnątrz przy użyciu sieci firewall.
e) Wykonywanie kopii awaryjnych danych na ……..
f) Ochronę sprzętu komputerowego wykorzystywanego u Administratora przed złośliwym oprogramowaniem.
g) Zabezpieczenie dostępu do urządzeń firmy przy pomocy haseł dostępu.
h) Wykorzystanie szyfrowania danych przy ich transmisji.
i) ……..
j) ……..
k) ……..
l) …….

ZAŁĄCZNIK: Lista kontrolna – pomocnicze pytania audytowe – identyfikacja danych osobowych

§13

NARUSZENIA ZASAD OCHRONY DANYCH OSOBOWYCH

1. Administrator stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych w terminie 72 godzin od stwierdzenia naruszenia.
2. W przypadku stwierdzenia naruszenia ochrony danych osobowych Administrator dokonuje oceny, czy zaistniałe naruszenie mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych.
3. W każdej sytuacji, w której zaistniałe naruszenie mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych, Administrator zgłasza fakt naruszenia zasad ochrony danych organowi nadzorczemu bez zbędnej zwłoki – jeżeli jest to wykonalne, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia.
4. Jeżeli ryzyko naruszenia praw i wolności jest wysokie, Administrator zawiadamia o incydencie także osobę, której dane dotyczą.
5. Poinformowania o naruszeniu organu nadzorczego i osoby, której dane dotyczą nie stosuje się, jeśli przepisy prawa krajowego wyłączają odpowiedzialność Administratora w tym zakresie.
6. Naruszenia nie zgłasza się organowi nadzorczemu, ani osobie, której dane dotyczą, jeśli Administrator jest w stanie wykazać małe prawdopodobieństwo naruszenia praw lub wolności osób fizycznych.
7. Wszystkie osoby upoważnione do przetwarzania danych osobowych są zobowiązane poinformować Administratora o ewentualnych naruszeniach bezpieczeństwa ochrony danych osobowych lub uzasadnionych podejrzeniach wystąpienia takiego naruszenia.
8. W przypadku jakiegokolwiek naruszenia ochrony danych osobowych Administrator sprawdza, dlaczego doszło do naruszenia i jakie środki zapobiegawcze wprowadzić.
9. W przypadku wystąpienia naruszenia w stosunku do danych, Administrator prowadzi Rejestr naruszeń stanowiący załącznik do Polityki.
10. Szczegółowe zasady postępowania zawierają:

ZAŁĄCZNIK: Instrukcja postępowania w przypadku wystąpienia incydentu związanego z naruszeniem ochrony danych osobowych

ZAŁĄCZNIK: Zgłoszenie incydentu naruszenia danych osobowych

ZAŁĄCZNIK: Rejestr naruszeń ochrony danych

§14
POWIERZENIE PRZETWARZANIA DANYCH OSOBOWYCH

1. Administrator Danych Osobowych może powierzyć przetwarzanie danych osobowych innemu podmiotowi wyłącznie w drodze umowy zawartej w formie dokumentowej (w tym także elektronicznej) zgodnie z wymogami wskazanymi dla takich umów w art. 28 RODO, lub poprzez akceptację regulaminu świadczonej usługi pomiędzy Administratorem a podmiotem trzecim, któremu dane się powierza w celu i w zakresie wykonania konkretnej czynności w imieniu Administratora.
2. Przed powierzeniem przetwarzania danych osobowych Administrator w miarę możliwości uzyskuje informacje o dotychczasowych praktykach procesora dotyczących zabezpieczenia danych osobowych.
3. Administrator powierza przetwarzane dane osobowe osób fizycznych, w szczególności w celu:
   a) prowadzenia obsługi w zakresie BHP,
   b) prowadzenia obsługi księgowej,
   c) serwisu i konserwacji urządzeń, na których znajdują się dane osobowe,
   d) usługi IT, administrowanie serwerem, hosting,
   e) usługi chmurowej,
   f) utrzymywania bazy danych subskrybentów w zewnętrznych bazach mailingowych i systemach do obsługi newslettera,
   g) inne (wymień jakie): ……..
4. Umowa powierzenia określa w szczególności cel i zakres powierzenia przetwarzania danych osobowych.
5. Administrator sprawuje kontrolę nad tym w jakim zakresie i w jakim celu powierza dane osobowe. Prowadzi w tym celu ewidencję podmiotów, którym dane zostały powierzone do przetwarzania.
6. Administrator powierza dane osobowe tylko tym podmiotom, które gwarantują zastosowanie środków organizacyjnych i technicznych, zabezpieczających dane przed dostępem osób nieupoważnionych na zasadach określonych w przepisach prawa.
7. Administrator prowadzi w odrębnym dokumencie Rejestr umów powierzenia.
8. Przed podpisaniem umowy powierzenia, Administrator bądź inna osoba wyznaczona:
   a) weryfikuje czy umowa powierzenia zawiera wszystkie elementy przewidziane art. 28 RODO,

b) weryfikuje czy nie zachodzi konieczność uwzględnienia dodatkowych zabezpieczeń w umowie (np. kary umowne itp.).

ZAŁĄCZNIK: Umowa powierzenia – wzór (jeśli dotyczy)

ZAŁĄCZNIK: Rejestr umów powierzenia (jeśli dotyczy)

§15
PRZEKAZYWANIE DANYCH DO PAŃSTWA TRZECIEGO

1. W przypadku gdy zachodzi przekazanie danych do państw trzecich poza UE/EOG, Administrator dokonuje przekazania bądź do podmiotów w ramach tzw. Tarczy Prywatności bądź też w oparciu o standardowe klauzule umowne lub bez ww. zabezpieczeń w oparciu o zgodę osoby, której dane dotyczącą lub też w oparciu o inne przesłanki przewidziane w RODO (m.in. niezbędność do zawarcia/realizacji umowy).
2. Szczegółowe wskazanie o przekazaniu danych do państw trzecich zawiera każdorazowo klauzula informacyjna.

§16
WSPÓŁADMINISTROWANIE

1. W przypadku gdy zachodzi współadministrowanie, tzn. poza Administratorem danych również inny podmiot decyduje o celach przetwarzania danych i środkach ich zabezpieczania, informacja o współadministrowaniu wskazywana jest w:
   1) klauzulach informacyjnych,
   2) rejestrze czynności przetwarzania,
2. W związku ze współadministrowaniem zawierana jest także umowa o współadministrowanie.

§17
MONITOROWANIE I AUDYTY

1. Administrator lub inna osoba wyznaczona lub wyspecjalizowany podmiot zewnętrzny przeprowadza audyt zgodności z przepisami i zasadami ochrony danych osobowych. Zaleca się, aby audyt był przeprowadzany przynajmniej raz na rok lub w razie potrzeby – częściej.
2. W ramach audytu dokonuje się weryfikacji w szczególności:

a. aktualności Polityki Ochrony Danych i załączników,
b. aktualności Analizy Ryzyka;
c. aktualności Rejestru czynności przetwarzania i kategorii przetwarzania(o ile wystąpi konieczność jego prowadzenia),
d. stosowania się pracowników i innych osób do przepisów prawa i wewnętrznych regulacji z zakresu ochrony danych,
e. poprawności przetwarzania danych osobowych,
f. potrzeby powołania Inspektora Ochrony Danych.

3. Z czynności kontrolnych sporządza się raport z kontroli lub w innej formie opisuje się przeprowadzoną kontrolę (np. notatka), w ramach którego poza zakresem czynności przeprowadzanych w ramach audytu wskazuje się także opis stanu przestrzegania przepisów i zasad, wskazuje się elementy wymagające zmiany/poprawy, opisuje się zalecenia.

§18
POSTANOWIENIA KOŃCOWE

1. Dokumentacja przetwarzania danych osobowych stanowi wewnętrzną regulację Administratora i obowiązuje wszystkich pracowników i współpracowników Administratora oraz inne osoby przetwarzające dane osobowe przetwarzane przez Administratora.
2. Wszyscy pracownicy, współpracownicy i osoby upoważnione do przetwarzania danych osobowych w imieniu Administratora są zobowiązani do zapoznania się i przestrzegania zasad, instrukcji i procedur wprowadzonej dokumentacji przetwarzania danych osobowych.
3. Za niedopełnienie obowiązków wynikających z niniejszego dokumentu osoby wymienione w ust. 1 ponoszą odpowiedzialność na podstawie Kodeksu pracy, Przepisów o ochronie danych osobowych, ustawy Kodeks karny oraz innych przepisów.
4. Dopuszcza się dokonywanie zmian w niniejszym dokumencie oraz dokumentach powiązanych tylko przez osoby upoważnione.
5. Zmiany w dokumencie Polityki oraz w załącznikach wprowadzane są w chwili pojawienia się ważnych okoliczności lub nowych przepisów prawnych, istotnych dla spójności i aktualności Polityki, bądź aktualizacji dotychczasowych przepisów dotyczących ochrony lub przetwarzania danych osobowych. Zmiany zatwierdzane są przez Administratora i podawane do wiadomości osób uczestniczących w przetwarzaniu danych osobowych poprzez

publikację w intranecie lub dokumentach formalnych udostępnianych w ustalony wewnętrznie sposób.

6. Integralną część niniejszej Polityki są wymienione w jej treści dokumenty i wzory, a także inne dokumenty mające na celu ochronę danych osobowych a wdrożone przez Administratora.

……

[data i podpis Administratora Danych Osobowych]