POLITYKA OCHRONY DANYCH OSOBOWYCH

JM PROFIT Jakub Markiewicz

1. Uwagi wstępne

Niniejszy dokument zatytułowany „Polityka ochrony danych osobowych" (dalej: Polityka) ma za zadanie stanowić mapę wymogów, zasad i regulacji ochrony danych osobowych w przedsiębiorstwie Jakuba Markiewicza działającego pod firmą JM PROFIT Jakub Markiewicz,ul. Narcyzowa 6, 63-004 Tulce, wpisana do rejestru przedsiębiorców w Centralnej Ewidencji i Informacji o Działalności Gospodarczej pod numerem NIP: 7822254960 (dalej: JM PROFIT Jakub Markiewicz).

Niniejsza Polityka jest polityką ochrony danych osobowych w rozumieniu RODO – rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzanie danych osobowych i w sprawie swobodnego przepływu takich danych (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119, s. 1).

Polityka zawiera:

a. opis zasad ochrony danych obowiązujących w JM PROFIT,
b. odwołania do załączników uszczegóławiających (wzorcowe procedury lub instrukcje dotyczące poszczególnych obszarów z zakresu ochrony danych osobowych wymagających doprecyzowania w odrębnych dokumentach).

Polityka wyznacza kierunek działania JM PROFIT Jakub Markiewicz oraz jej pracowników w celu zapewniania systemowego nadzoru nad gromadzeniem, przetwarzaniem, przechowywaniem i udostępnianiem informacji.

2. Definicje

Administrator (ADO) – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.

Analiza ryzyka – proces identyfikowania dla danego środowiska przetwarzania zagrożeń i oszacowanie potencjalnych skutków ich wystąpienia, a następnie wyszukanie i zaproponowanie środków technicznych i organizacyjnych redukujących prawdopodobieństwo i/lub skutki ich wystąpienia.

Anonimizacja - to nieodwracalne przetworzenie danych osobowych w taki sposób, by nie można ich było przypisać konkretnej osobie. Anonimizacja ma na celu uniemożliwienie identyfikacji osób, których dane zostały poddane temu procesowi.

Czynność przetwarzania danych – to mniejszy lub większy wycinek procesu przetwarzania danych realizowanego w konkretnym celu przetwarzania danych. (zbierania, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, modyfikowanie, adaptowanie, pobieranie, przeglądanie, wykorzystywanie, rozpowszechnianie, usuwanie lub niszczenie)

Dane osobowe – oznaczają informację o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. (data urodzenia, adres zamieszkania, kolor oczu, waga, poglądy)

Inspektor ochrony danych to funkcja zdefiniowana w art. 37-39 RODO. Zadaniem inspektora jest dbanie o ochronę danych w organizacji. Inspektor ochrony danych nie odpowiada za zgodność organizacji z RODO.

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

Ocena skutków ochrony danych (DPIA) – sformalizowana analiza ryzyka przetwarzania danych osobowych dla sytuacji, w których to ryzyko zostało ustalone jako wysokie. Zgodnie z art. 35 RODO przeprowadzenie DPIA będzie wymagane dla wszystkich zmian technologicznych, biznesowych, organizacyjnych w danej organizacji, materializujących się po 25 maja 2018 r., które mogą powodować wysokie ryzyko naruszenia praw lub wolności osób, których dane są przetwarzane.

Odbiorca – osoba fizyczną lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego czy jest stroną trzecią. (inny administrator, osoby powiązane z administratorem)

Ograniczenie przetwarzania – wskutek ograniczenia administrator może dane posiadać oraz wykonywać tylko te operacje, na które zgadza się podmiot danych, a niezależnie takie, które są potrzebne do sporów lub ochrony praw innego podmiotu, lub gdy zachodzi ważny interes publiczny.

Przetwarzanie – oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, przeglądanie, modyfikowanie, usuwanie.

Pseudonimizacja to zastępowanie identyfikatorów (imię, nazwisko, PESEL) pseudonimami, czyli unikalnymi dla danej osoby kodami, liczbami lub obrazami, które nie mają rzeczywistego powiązania z daną osobą.

Rejestr czynności przetwarzania danych stanowi formę dokumentowania czynności przetwarzania danych i jest jednym z kluczowych elementów umożliwiających realizację fundamentalnej zasady, na której opiera się cały system ochrony danych osobowych, czyli zasady rozliczalności.

Ryzyko – ryzyko naruszenia praw lub wolności osób, a więc skutek w postaci szkody dla osoby, której dane dotyczą.

Podmiot przetwarzający – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę, lub inny podmiot, który przetwarza dane osobowe w imieniu administratora. Podmiot przetwarzający musi wykonywać operacje przetwarzania na udokumentowane polecenie

administratora danych w imieniu administratora. (Typowe funkcje podmiotów przetwarzających to: zewnętrzna obsługa kadrowo-placowa, księgowa, podatkowa, informatyczna)

3. Obowiązki ADO w zakresie przetwarzania danych osobowych.

a) Obowiązek legalnego przetwarzania danych osobowych

W każdej sytuacji przetwarzania danych osobowych muszą istnieć przesłanki legalizujące przetwarzanie danych osobowych. Przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy - i w takim zakresie, w jakim - spełniony jest co najmniej jeden z poniższych warunków:

I. osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
II. przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
III. przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
IV. przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
V. przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
VI. przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności, gdy osoba, której dane dotyczą, jest dzieckiem.

Przetwarzanie jest zabronione w przypadku danych osobowych tzw. szczególnych kategorii danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby oraz danych dotyczących wyroków skazujących oraz naruszeń prawa lub powiązanych środków bezpieczeństwa

Przetwarzanie szczególnych kategorii danych osobowych jest jednak dopuszczalne m.in. jeżeli:

I. osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach;
II. przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej;
III. przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody;
IV. przetwarzania dokonuje się w ramach uprawnionej działalności prowadzonej z zachowaniem odpowiednich zabezpieczeń przez fundację, stowarzyszenie lub inny

niezarobkowy podmiot o celach politycznych, światopoglądowych, religijnych lub związkowych, pod warunkiem że przetwarzanie dotyczy wyłącznie członków lub byłych członków tego podmiotu lub osób utrzymujących z nim stałe kontakty w związku z jego celami oraz że dane osobowe nie są ujawniane poza tym podmiotem bez zgody osób, których dane dotyczą;

V. przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą;

VI. przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy;

VII. przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą;

VIII. przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego;

IX. przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, na podstawie prawa Unii lub prawa państwa członkowskiego, które przewidują odpowiednie, konkretne środki ochrony praw i wolności osób, których dane dotyczą, w szczególności tajemnicę zawodową;

X. przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie, konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą.

b) Obowiązek informacyjny o przetwarzaniu danych osobowych

Na administratorze danych spoczywa także obowiązek sprawdzenia, czy prawa osób, których dane dotyczą są respektowane. Podczas pozyskiwania danych od osoby, administrator powinien przekazać następujące informacje (art. 13 ust. 1 i 2 RODO):

- informacje podstawowe:
    - tożsamość i dane kontaktowe administratora,
    - cele przetwarzania danych oraz podstawa prawna dla każdego celu,
    - prawnie uzasadnione interesy realizowane przez administratora lub przez stronę trzecią,
    - informacje o odbiorcach danych osobowych lub ich kategoriach,
    - okres przechowywania danych;
- informacje o prawach osoby, której dane dotyczą, tj. o prawie do:
    - dostępu do danych
    - sprostowania
    - usunięcia
    - ograniczenia przetwarzania
    - sprzeciwu

    - przenoszenia danych
    - skargi do organu nadzorczego
    - cofnięcia zgody
- informacje czy podanie danych jest:
    - wymogiem ustawowym/umownym zawarcia umowy,
    - obowiązkowe,
    - jakie są konsekwencje niepodania danych.

Wzór klauzuli informacyjnej realizującej powyższy obowiązek znajduje się w załączniku nr 1.

Wzór klauzuli zgody na przetwarzanie danych zwykłych stanowi załącznik nr 16.

Wzór klauzuli zgody na przetwarzanie danych szczególnych kategorii stanowi załącznik nr 17.

Podanych wyżej zasad nie stosuje się, jeżeli przepis innej ustawy zezwala na przetwarzanie danych bez ujawniania faktycznego celu ich zbierania lub jeżeli osoba, której dane dotyczą, posiada już te informacje.

c) Pozostałe zasady dotyczące przetwarzania danych osobowych

Dane osobowe muszą być:

I. przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość");
II. zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; („ograniczenie celu");
III. adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych");
IV. prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („prawidłowość");
V. przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne w celu ochrony praw i wolności osób, których dane dotyczą („ograniczenie przechowywania");
VI. przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność").

Administrator jest odpowiedzialny za przestrzeganie wyżej wskazanych zasad i musi być w stanie wykazać ich przestrzeganie („rozliczalność").

d) Obowiązki przy powierzeniu przetwarzania danych osobowych

W sytuacji, gdy zaistnieje konieczność przetwarzania danych osobowych przez podmioty, które świadczą usługi dla Administratora danych, istnieje możliwość powierzenia przetwarzania danych osobowych.

Zgodnie z art. 28 ust. 2 RODO powierzenie przetwarzania danych, a także podpowierzanie, wymaga pisemnej (w tym elektronicznej) umowy lub innego instrumentu prawnego między administratorem a podmiotem przetwarzającym.

Podmiot, któremu powierzono do przetwarzania dane osobowe, może przetwarzać te dane wyłącznie w zakresie i celu przewidzianym w umowie.

Jeżeli do wykonania w imieniu administratora konkretnych czynności przetwarzania podmiot przetwarzający korzysta z usług innego podmiotu przetwarzającego, na ten inny podmiot przetwarzający nałożone zostają te same obowiązki ochrony danych jak w umowie lub innym akcie prawnym między administratorem a podmiotem przetwarzającym, w szczególności obowiązek zapewnienia wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych. Jeżeli ten inny podmiot przetwarzający nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, pełna odpowiedzialność wobec administratora za wypełnienie obowiązków tego innego podmiotu przetwarzającego spoczywa na pierwotnym podmiocie przetwarzającym.

ADO może powierzyć do przetwarzania podmiotowi trzeciemu pod warunkiem spisania umowy powierzenia danych osobowych, np.: podmiotowi prowadzącemu sprawy BHP; podmiotowi wykonującemu usługi księgowo-finansowe, kadrowo-płacowe, firmom/osobom serwisującym systemy informatyczne, podmiotom archiwizującym czy niszczącym dokumentację papierową lub elektroniczną.

ADO ma obowiązek uzyskać od osób biorących udział w przetwarzaniu zobowiązania do przestrzegania tajemnicy, chyba że osoby te są objęte obowiązkiem ustawowym do zachowania tajemnicy.

Administrator koordynuje prace związane z opracowaniem i zawarciem umów powierzania danych osobowych w JM PROFIT i prowadzi Rejestr powierzeń zbiorów danych osobowych. (Załącznik nr 2)

Wzór umowy powierzania przetwarzania danych osobowych stanowi Załącznik nr 3.

Wzór oświadczenia o zachowaniu poufności stanowi Załącznik nr 4.

e) Respektowanie praw osoby, której dane dotyczą

Osoba, której dane dotyczą, jest uprawniona do uzyskania od administratora potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz następujących informacji:

I. cele przetwarzania;
II. kategorie odnośnych danych osobowych;
III. informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;
IV. w miarę możliwości planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
V. informacje o prawie do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania;
VI. informacje o prawie wniesienia skargi do organu nadzorczego;

VII. jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle;
VIII. informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

Administrator danych obowiązany jest w terminie 30 dni poinformować osobę, której dane dotyczą o przysługujących jej prawach oraz udzielić w/w informacji.

Administrator obowiązany jest do poinformowania o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania, każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. Administrator informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.

Osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego usunięcia dotyczących jej danych osobowych, a administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, jeżeli zachodzi jedna z następujących okoliczności:

I. dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
II. osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie i nie ma innej podstawy prawnej przetwarzania;
III. osoba, której dane dotyczą, wnosi sprzeciw wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania;
IV. dane osobowe były przetwarzane niezgodnie z prawem;
V. dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator;
VI. dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego;

f) Obowiązek zabezpieczenia danych osobowych.

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

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

Administrator danych osobowych prowadzi dokumentację z zakresu ochrony danych osobowych, tj. Politykę ochrony danych osobowych.

4. Sankcje karne

Zgodnie z art. 83 RODO - Każdy organ nadzorczy zapewnia, by stosowane na mocy niniejszego artykułu za naruszenia niniejszego rozporządzenia administracyjne kary pieniężne, były w każdym indywidualnym przypadku skuteczne, proporcjonalne i odstraszające.

Administracyjne kary pieniężne nakłada się, zależnie od okoliczności każdego indywidualnego przypadku. Organ administracyjny decydując, czy nałożyć administracyjną karę pieniężną, oraz ustalając jej wysokość, zwraca w każdym indywidualnym przypadku należytą uwagę na:

a) charakter, wagę i czas trwania naruszenia przy uwzględnieniu charakteru, zakresu lub celu danego przetwarzania, liczby poszkodowanych osób, których dane dotyczą, oraz rozmiaru poniesionej przez nie szkody;

b) umyślny lub nieumyślny charakter naruszenia;

c) działania podjęte przez administratora lub podmiot przetwarzający w celu zminimalizowania szkody poniesionej przez osoby, których dane dotyczą;

d) stopień odpowiedzialności administratora lub podmiotu przetwarzającego z uwzględnieniem środków technicznych i organizacyjnych wdrożonych przez nich;

e) wszelkie stosowne wcześniejsze naruszenia ze strony administratora lub podmiotu przetwarzającego;

f) stopień współpracy z organem nadzorczym w celu usunięcia naruszenia oraz złagodzenia jego ewentualnych negatywnych skutków;

g) kategorie danych osobowych, których dotyczyło naruszenie;

h) sposób, w jaki organ nadzorczy dowiedział się o naruszeniu, w szczególności, czy i w jakim zakresie administrator lub podmiot przetwarzający zgłosili naruszenie;

i) jeżeli wobec administratora lub podmiotu przetwarzającego, których sprawa dotyczy, zostały wcześniej zastosowane w tej samej sprawie środki, o których mowa w art. 58 ust. 2 RODO – przestrzeganie tych środków;

j) stosowanie zatwierdzonych kodeksów postępowania lub zatwierdzonych mechanizmów certyfikacji;

k) oraz wszelkie inne obciążające lub łagodzące czynniki mające zastosowanie do okoliczności sprawy, takie jak osiągnięte bezpośrednio lub pośrednio w związku z naruszeniem korzyści finansowe lub uniknięte straty.

Naruszenia przepisów dotyczących następujących kwestii podlegają administracyjnej karze pieniężnej w wysokości do 10 000 000 EUR lub do 20 000 000 EUR, a w przypadku przedsiębiorstwa – w wysokości do 2 % lub do 4 % jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego.

5. Zagrożenia bezpieczeństwa danych osobowych

Wybór zabezpieczeń fizycznych, technicznych i organizacyjnych jest poprzedzany analizą ryzyka. Procedura analizy ryzyka stanowi **załącznik nr 5** do niniejszej dokumentacji.

Pracownicy JM PROFIT zobowiązani do stosowania *Procedury postępowania w sytuacji wykrycia naruszenia ochrony danych osobowych,* tj.:

- Pracownicy niezwłocznie zgłaszają Administratorowi stwierdzenie wystąpienia naruszenia ochrony danych osobowych
- W przypadku istnienia takiej możliwości, zaleca się zabezpieczenie danych osobowych na czas przybycia wskazanych osób, nie zacierając ewentualnych śladów naruszeń na potrzeby oględzin przez Policję.
- Administrator każdorazowo w sytuacjach naruszenia zasad ochrony danych tworzy raport i odnotowuje wystąpienie naruszenia w Rejestrze naruszeń ochrony danych osobowych. (Załącznik nr 6, Załącznik nr 7)
- Wobec pracowników winnych naruszenia bezpieczeństwa informacji na skutek nieprzestrzegania zasad, może zostać wszczęte postępowanie dyscyplinarne.
- Przyczyny naruszeń będą omawiane podczas szkoleń dla pracowników, aby w przyszłości wykluczyć wystąpienie podobnych incydentów.

A. Rejestr czynności przetwarzania

Zgodnie z art. 30 RODO – Administrator oraz przedstawiciel administratora prowadzą rejestr czynności przetwarzania danych osobowych, za które odpowiadają. W rejestrze tym zamieszcza się wszystkie następujące informacje:

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

Za prowadzenie rejestru czynności przetwarzania odpowiedzialny jest Administrator.

B. Środki organizacyjne niezbędne do zapewnienia zgodności przetwarzania z zasadami przetwarzania danych wskazanymi w art. 5 Rozporządzenia

Polityka ochrony danych osobowych obowiązuje wszystkich pracowników, stażystów, praktykantów oraz osoby fizyczne, prawne i jednostki organizacyjne nieposiadające osobowości prawnej, którym ustawa przyznaje zdolność prawną, z którymi JM PROFIT zawarła umowę, jeżeli z umowy wynika, że będą posiadały dostęp do zasobów informacyjnych JM PROFIT.

Wszystkie osoby oraz podmioty wyżej wskazane są zapoznane z niniejszą dokumentacją i potwierdzają ten fakt stosownym oświadczeniem. (Załącznik nr 8)

C. Obowiązki pracowników.

Pracownicy zobowiązani są do przetwarzania danych zgodnie z wytycznymi w niniejszej dokumentacji.

Pracownicy zobowiązani są do wskazywania podstawy prawnej przetwarzania danych osobowych w konkretnym, realizowanym przez siebie celu. Jeśli jedyną podstawą prawną jest zgoda osoby (której dane dotyczą), pracownik ma w obowiązku zadbać o udokumentowanie tej zgody na piśmie.

W JM PROFIT cyklicznie organizowane są szkolenia z zakresu ochrony danych osobowych w celu zapoznania osób nieupoważnionych do przetwarzania danych osobowych z przepisami prawa oraz zasadami przyjętymi w niniejszej dokumentacji. Pracownicy zobowiązani są do uczestnictwa w szkoleniu.

Każdy z pracowników posiada pisemne upoważnienie do przetwarzania w imieniu administratora udostępnionych mu danych osobowych. Wzór upoważnienia stanowi załącznik nr 10.

Upoważnienia dla byłych pracowników JM PROFIT są niezwłocznie po zakończeniu stosunku pracy odwoływane. Odwołanie upoważnienia do przetwarzania danych osobowych stanowi załącznik nr 11.

D. Procedura dotycząca organizacji stanowiska pracy osoby upoważnionej do przetwarzania danych osobowych.

Pracownik jest obowiązany ustawić ekran monitora komputerowego tak, by osoby niepowołane nie mogły oglądać wyświetlanych w nim treści.

Pracownik jest zobowiązany do niepozostawiania bez kontroli dokumentów, nośników z danymi osobowymi i sprzętu komputerowego w miejscach niezabezpieczonych na terenie JM PROFIT.

Komputery osobiste i stacjonarne nie mogą być pozostawiane bez nadzoru, w stanie zalogowania do systemu teleinformatycznego. Niedopuszczalne jest zakończenie pracy bez wykonania pełnej i poprawnej procedury zamknięcia systemu.

Zabrania się pozostawiania osób postronnych w pomieszczeniu, w którym przetwarzane są dane osobowe, bez obecności osoby upoważnionej do przetwarzania danych osobowych.

Wynoszenie dokumentacji z danymi osobowymi, nośników oraz komputerów przenośnych (laptopów) poza obszar przetwarzania danych osobowych jest możliwe tylko za zgodą bezpośredniego przełożonego.

Podczas wynoszenia dokumentacji, nośników z danymi osobowymi oraz laptopów przenośnych pracownik jest zobowiązany do zachowania szczególnej ostrożności i zastosowanie zabezpieczeń (m.in. nie pozostawiać wymienionych przedmiotów w samochodzie, nie udostępniać członkom rodziny).

W przypadku utraty lub kradzieży komputera przenośnego, należy to natychmiast zgłosić Administratorowi oraz poinformować policję o popełnieniu przestępstwa.

Uruchomienie komputera powinno być zabezpieczone hasłem. Zabrania się wymiany między pracownikami identyfikatorów i haseł do systemu informatycznego, celem wykonania operacji w zastępstwie osoby odpowiedzialnej.

Wprowadza się zasadę „czystego biurka”, która oznacza uniemożliwienie zapoznania się z danymi osobowymi osobom nieupoważnionym, a także w razie możliwości zamykanie w szafkach/biurkach dokumentacji z danymi osobowymi oraz wszelkich nośników tych informacji.

Odpowiedzialność za właściwe użytkowanie sprzętu służącego do przetwarzania informacji spoczywa na jego użytkowniku.

Niszczenie dokumentacji papierowej odbywa się w niszczarce.

Pracownicy mogą przetwarzać dane osobowe poza godzinami pracy jedynie po uzyskaniu zezwolenia bezpośredniego przełożonego.

Zabrania się pozostawiania we wspólnych drukarkach dokumentów z danymi osobowymi.

Procedura organizacji stanowiska osoby upoważnionej do przetwarzania danych stanowi załącznik nr 12.

E. Środki techniczne ochrony danych osobowych.

Zbiory danych osobowych przetwarzane. W JM PROFIT zabezpieczone są przez wdrożenie poniżysz środków technicznych.

Środki sprzętowe, infrastruktury informatycznej i telekomunikacyjnej:

- zastosowano środki ochrony przed szkodliwym oprogramowaniem takim jak np. robaki, wirusy, konie trojańskie, rootkity itp., w postaci oprogramowania antywirusowego.
- Użyto systemy firewall chroniącego przed atakiem z sieci publicznej.

Środki ochrony w ramach systemowych narzędzi programowych i baz danych:

- wymagane jest uwierzytelnianie użytkownika stacji roboczej poprzez podanie loginu i hasła domowego;
- dostęp do zbiorów danych osobowych wymaga uwierzytelniania z wykorzystaniem identyfikatora użytkownika i hasła;
- zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.

SPIS ZAŁĄCZNIKÓW

1. Wzór klauzuli informacyjnej.
2. Rejestr powierzeń zbiorów danych osobowych.
3. Wzór umowy powierzania przetwarzania danych osobowych.
4. Wzór oświadczenia o zaufaniu poufności.
5. Procedura analizy ryzyka.
6. Wzór raportu z naruszenia ochrony danych osobowych.
7. Rejestr naruszeń ochrony danych osobowych.
8. Wzór oświadczenia o zapoznaniu się z polityką ochrony danych osobowych.
9. Wzór sprawozdania z kontroli zgodności przetwarzania danych osobowych z RODO.

10. Wzór upoważnienia do przetwarzania danych osobowych.
11. Wzór odwołania upoważnienia do przetwarzania danych osobowych.
12. Procedura organizacji stanowiska osoby upoważnionej do przetwarzania danych.
13. Rejestr osób upoważnionych do przetwarzania danych osobowych.
14. Wzór wniosku o udzielenie informacji o danych ze zbioru danych osobowych w JM PROFIT;
15. Klauzula zgody na przetwarzanie danych zwykłych.