POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

w firmie Madam Events Tomasz Mazurkiewicz
prowadzącą catering o nazwie:

Madam Catering

adres siedziby:

ul. Św. U. Ledóchowskiej 5h/18, 02-972 Warszawa

Spis treści

I WPROWADZENIE

Polityka Bezpieczeństwa Danych Osobowych, zwana dalej Polityką, została sporządzona w związku z wymaganiami 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 (ogólne rozporządzenie o ochronie danych) oraz innych wcześniejszych aktów prawnych takich jak ustawa z dnia 29 sierpnia 1997r. o ochronie danych osobowych oraz późniejszymi uzupełnieniami wynikającymi z rozporządzeń Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (U. 2004 nr 100 poz. 1024).

Niniejszy dokument stanowi zbiór spójnych, precyzyjnych reguł i procedur, według których catering dietetyczny buduje, zarządza oraz udostępnia zasoby i systemy informacyjne. Ustanawia przewidziane do wykonania działania oraz sposób ustanowienia zasad i reguł postępowania koniecznych do zapewnienia właściwej ochrony przetwarzanych danych osobowych. Polityka ustanawia zasady bezpieczeństwa przetwarzania danych osobowych, które powinny być przestrzegane i stosowane w cateringu dietetycznym przez wszystkie osoby przetwarzające dane osobowe, wraz z powołaniem na właściwe podstawy prawne. Polityka reguluje zasady organizacji pracy przy zbiorach danych osobowych przetwarzanych w systemach informatycznych oraz metodami tradycyjnymi. Opisano w niej również zagrożenia bezpieczeństwa przetwarzanych danych osobowych oraz sposoby reakcji na przypadki naruszeń bezpieczeństwa.

Niniejszy dokument pełni również funkcję informacyjną i edukacyjną, poprzez zaprezentowanie obowiązków i odpowiedzialności osób związanych z przetwarzaniem danych osobowych. Każdy z pracowników cateringu dietetycznego powinien się z Polityką Bezpieczeństwa Danych Osobowych.

Catering dietetyczny stosuje adekwatne do sytuacji środki aby zapewnić bezpieczeństwo informacji.

Catering dietetyczny wypełnia obowiązki nałożone przez 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 wraz z późniejszymi zmianami, w szczególności poprzez:

1. wykonanie dokumentacji opisującej środki organizacyjne i techniczne służące ochronie przetwarzanych danych osobowych,
2. przestrzeganie obowiązku informacyjnego wypełnianego przy zbieraniu danych osobowych
3. szczególną staranność przy przetwarzaniu danych osobowych w celu ochrony interesów osób, których dane przetwarza,
4. udzielanie informacji o zakresie przetwarzanych danych osobowych,
5. przestrzeganie obowiązku uzupełniania, uaktualnienia, sprostowania danych, czasowego lub stałego wstrzymania przetwarzania kwestionowanych danych lub ich usunięcia ze zbioru, gdy zażąda tego osoba, której dane są przetwarzane przez administratora,

6. przestrzeganie obowiązku stosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną,
7. dopuszczenie do przetwarzania danych wyłącznie osób posiadających upoważnienie nadane przez administratora danych,
8. bieżącą kontrolę, jakie dane, kiedy i przez kogo są przetwarzane i komu są przekazywane,
9. prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych.

Uzupełnieniem i dopełnieniem niniejszej Polityki jest Instrukcja zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych (zał. nr 1), ustanawiająca sposób zarządzania systemami informatycznymi, służącymi do przetwarzania danych osobowych w cateringu dietetycznym.

II PODSTAWA PRAWNA

Zasady przetwarzania danych osobowych w szczególności regulują:

- ✓ 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 (ogólne rozporządzenie o ochronie danych)
- ✓ Ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997 r.
- ✓ Rozporządzenie Prezydenta Rzeczypospolitej Polskiej z dnia 3 listopada 2006 r. w sprawie nadania statutu Biuru Generalnego Inspektora Ochrony Danych Osobowych – wydane na podstawie art. 13 ust. 3 ustawy,
- ✓ Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 22 kwietnia 2004 r. w sprawie wzorów imiennego upoważnienia i legitymacji służbowej inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych – wydane na podstawie art. 22a ustawy,
- ✓ Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych – wydane na podstawie art. 39a ustawy,
- ✓ Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych – wydane na podstawie art. 46a ustawy,
- ✓ Ustawa o świadczeniu usług drogą elektroniczną,
- ✓ Wytyczne w zakresie opracowania i wdrożenia polityki bezpieczeństwa Generalnego Inspektora Ochrony Danych Osobowych.
- ✓ Rozporządzenie Ministra Administracji i Cyfryzacji z 10 grudnia 2014 r. w sprawie wzorów zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji,
- ✓ Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych,
- ✓ Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych,

III SŁOWNICZEK

ADO – Administrator Danych Osobowych, czyli właściciel cateringu dietetycznego lub osoba fizyczna przez niego wyznaczona decydująca o celach i środkach przetwarzania danych osobowych.

Dane osobowe - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, jeżeli jej 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. Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.

Dane wrażliwe - dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących wskazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.

GIODO – Generalny Inspektor Ochrony Danych Osobowych, będący organem powołanym do spraw z zakresu ochrony danych osobowych**.**

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 (ogólne rozporządzenie o ochronie danych)

Podmiot – Catering dietetyczny wskazany na pierwszej tytułowej stronie Polityki, dla celów którego niniejsza Polityka zostaje opracowana i wdrożona**.**

Polityka – niniejszy dokument Polityki Bezpieczeństwa Danych Osobowych.

Przetwarzanie danych – jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie.

Rozporządzenie – Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

System informatyczny – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

Upoważniony – osoba posiadająca formalne upoważnienie wydane przez Administratora Danych Osobowych lub przez osobę wyznaczoną, uprawniona do przetwarzania danych osobowych.

Ustawa – Ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997 r. ze zmianami.

Usuwanie danych –zniszczenie danych osobowych lub ich modyfikacja, która uniemożliwia ustalenie tożsamości osoby, której dane dotyczą.

Zabezpieczenie danych w systemie informatycznym –wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem

Zbiór danych – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

Zgoda osoby, której dane dotyczą – oświadczenie woli, którego treść stanowi zgoda na przetwarzanie danych osobowych osoby składającej oświadczenie. Zgoda nie może być dorozumiana z oświadczenia woli o innej treści, ani domniemana.

IV PRZETWARZANIE DANYCH OSOBOWYCH

Dane osobowe

Za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Przy rozstrzyganiu czy określona informacja lub informacje stanowią dane osobowe, Podmiot dokonuje zindywidualizowanej oceny, przy uwzględnieniu konkretnych okoliczności oraz rodzaju środków czy metod potrzebnych w określonej sytuacji do identyfikacji osoby.

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 (art. 1 ust. 2 ustawy oraz art. 1 ust. 1 RODO). Stosownie do ust. 3 powołanego przepisu, informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu i działań. Danymi osobowymi będą zatem zarówno takie dane, które pozwalają na określenie tożsamości konkretnej osoby, jak i takie, które nie pozwalają na jej natychmiastową identyfikację, ale są, przy pewnym nakładzie kosztów, czasu i działań, wystarczające do jej ustalenia.

Przetwarzanie danych osobowych

Przetwarzaniem danych osobowych są jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.

Przetwarzanie danych osobowych jest dopuszczalne tylko wtedy gdy:

1. Osoba, której dane dotyczą, wyrazi na to zgodę, chyba że chodzi o usunięcie dotyczących jej danych. Zgoda może obejmować również przetwarzanie danych w przyszłości, jeżeli nie zmienia

się cel przetwarzania. Zgoda nie może być domniemana lub dorozumiana. Jeżeli przetwarzanie danych jest niezbędne dla ochrony żywotnych interesów osoby, której dane dotyczą, a uzyskanie zgody nie jest możliwie, można przetwarzać dane bez zgody tej osoby, do czasu, gdy uzyskanie zgody będzie możliwe.
2. Jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa.
3. Jest to konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą.
4. Jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego.
5. Jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez Administratora danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą. Za prawnie usprawiedliwiony cel uważa się w szczególności: marketing bezpośredni własnych produktów lub usług administratora danych oraz dochodzenie roszczeń z tytułu prowadzonej działalności gospodarczej.

Madam Catering nie przetwarza danych wrażliwych (sensytywnych), z wyjątkiem sytuacji gdy przetwarzanie jest prowadzone w celu ochrony stanu zdrowia na przykład alergii pokarmowych klienta.

Obowiązki informacyjne o przetwarzaniu danych

W przypadku zbierania danych od osoby, której te dane dotyczą Administrator Danych Osobowych jest zobowiązany poinformować tę osobę o:

1. adresie swojej siedziby i pełnej nazwie,
2. celu zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych,
3. prawie dostępu do treści swoich danych oraz ich poprawiania,
4. dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.

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.

W przypadku zbierania danych nie od osoby, której te dane dotyczą Administrator Danych Osobowych jest zobowiązany poinformować tę osobę bezpośrednio po utrwaleniu danych o:

1. adresie swojej siedziby i pełnej nazwie,
2. celu i zakresie zbierania danych, a w szczególności o odbiorcach lub kategoriach odbiorców danych,
3. źródle danych,
4. prawie dostępu do treści swoich danych oraz ich poprawiania,
5. prawie wniesienia, pisemnego, umotywowanego żądania zaprzestania przetwarzania jej danych ze względu na jej szczególną sytuację,
6. prawie wniesienia sprzeciwu wobec przetwarzania jej danych w przypadkach, gdy Administrator Danych Osobowych zamierza je przetwarzać w celach marketingowych lub wobec przekazywania jej danych osobowych innemu administratorowi danych.

Podanych wyżej zasad nie stosuje się, jeżeli:

1. dane są przetwarzane przez Administratora Danych Osobowych na podstawie przepisów prawa,
2. przepis innej ustawy przewiduje lub dopuszcza zbieranie danych osobowych bez wiedzy osoby, której dane dotyczą,
3. dane te są niezbędne do badań naukowych, dydaktycznych, historycznych, statystycznych lub badania opinii publicznej, ich przetwarzanie nie narusza praw lub wolności osoby, której dane dotyczą, a spełnienie obowiązku informacyjnego wymagałoby nadmiernych nakładów lub zagrażałoby realizacji celu badania.

Zgodność przetwarzania z prawem

Catering dietetyczny realizuje obowiązki ustanowione w art. 26 i 36 ustawy oraz artykule 6 ust.1 RODO poprzez dołożenie szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, zapewniając aby dane te były:

1. **przetwarzane zgodnie z prawem,**

   (Zgodne z wszelkimi normami prawa, zarówno tymi już istniejącymi w momencie wejścia w życie ustawy i RODO, jak i tymi, które dopiero później zostały wprowadzone do porządku prawnego. Zgodność z prawem dotyczy przestrzegania zarówno przepisów prawa materialnego, jak i przepisów dotyczących postępowania).

2. **zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami,**

3. **przetwarzanie za zgodą**

   (Osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów w tym niezbędne przetwarzanie w celu do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy)

4. **merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane,**

   (Informacje wynikające z danych przetwarzanych przez administratora są zgodne z prawdą, kompletne oraz odpowiadają aktualnemu stanowi rzeczy. Administrator Danych Osobowych przetwarza dane tylko w takim zakresie, w jakim jest to niezbędne do wypełnienia celu, w jakim dane są przez niego przetwarzane).

5. **przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.**

6. administrator Danych Osobowych **stosuje środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną**, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

Dodatkowo catering dietetyczny zapewnia bezpieczeństwo informacji poprzez:

1. **poufność informacji**
   (informacje nie są udostępniane lub wyjawiane osobom nieupoważnionym, osoby nieuprawnione nie mają dostępu do danych),
2. **integralność informacji**
   (informacje są kompletne i niezmieniane w sposób nieuprawniony),
3. **rozliczalność działań**
   (wszystkie istotne czynności wykonane przy przetwarzaniu danych zostały zarejestrowane i jest możliwe zidentyfikowanie osoby, która daną czynność wykonała),
4. **niezawodność działań**
   (wykonywane czynności prowadzi do zamierzonych skutków),

Powierzenie przetwarzania danych

W przypadku konieczności przetwarzania danych przez odrębne podmioty świadczące usługi dla Administratora Danych Osobowych może on powierzyć ich przetwarzanie, w drodze umowy zawartej na piśmie.

1. Umowa powierzenia danych osobowych ustanawia w szczególności zakres i cel przetwarzania danych, a także zakres odpowiedzialności podmiotu, któremu powierzono przetwarzanie danych z tytułu jej niewykonania lub nienależytego wykonania.
2. Umowa powierzenia danych osobowych oraz jej realizacja muszą zachowywać zgodność z przepisami RODO. Podmiot zewnętrzny, któremu dane mają zostać powierzone, jest obowiązany do podjęcia środków zabezpieczających zbiór danych przed rozpoczęciem ich przetwarzania.
3. Umowa powierzenia danych osobowych uwzględnia zobowiązanie podmiotu trzeciego do przestrzegania niniejszej Polityki oraz przepisów powszechnie obowiązującego prawa.
4. Zawarcie umowy powierzenia danych osobowych nie skutkuje wyłączeniem odpowiedzialności cateringu dietetycznego za przetwarzanie danych osobowych w sposób niezgodny z przepisami prawa powszechnie obowiązującego.
5. Administrator Danych Osobowych prowadzi dokument Ewidencji podmiotów, którym catering powierza dane osobowe (zał. nr 4).

Z komentarzem [P1]: To jest załącznik, w którym wymieniacie wszystkie firmy (MasterLife, Księgowe, kurierów lub jakiekolwiek osoby nie będące zatrudnione bezpośrednio przez Was na podstawie umowy cywilno-prawnej

Powierzenie przetwarzania danych nie polega na udostępnieniu danych. Udostępnienie jest przekazaniem danych innemu podmiotowi (odbiorcy danych), który staje się ich administratorem zaś powierzenie polega na przetwarzaniu danych przez podmiot, który nie jest administratorem tych danych**.**

Udostępnianie danych

Z komentarzem [P2]: Podmiotami, które najczęściej zwracają się z wnioskiem o udostępnienie danych osobowych są np. osoby lub przedsiębiorstwa dochodzące swoich praw przed sądem, instytucje takie jak banki, ośrodki pomocy społecznej, czy ZUS, a także organy ścigania – Policja i Prokuratura.

Udostępnianie danych osobowych, zgodnie z RODO, jest jedną z form ich przetwarzania. Udostępnianie danych osobowych można określić, jako wszelkie działania umożliwiające innym niż administrator podmiotom, zapoznanie się z nimi.

1. Nie jest istotne czy udostępnianie danych ma charakter odpłatny czy nie, aby czynność była uznana za udostępnianie.

2. Nie jest istotne, czy udostępnianie następuje w formie przekazu ustnego, pisemnego, za pomocą powszechnych środków przekazu lub poprzez sieć komputerową itd., aby czynność była uznana za udostępnianie.
3. Udostępnianie danych osobowych osobom lub podmiotom uprawnionym do ich otrzymania odbywa się na mocy przepisów prawa.
4. Dane osobowe, z wyłączeniem danych wrażliwych, mogą być udostępniane nie w oparciu o przepisy prawa, jeżeli osoba wnioskująca w sposób wiarygodny uzasadni potrzebę posiadania tych danych, a ich udostępnienie nie naruszy praw i wolności osób, których dane dotyczą.
5. Dane osobowe udostępnia się na pisemny, umotywowany wniosek, chyba że przepis innej ustawy stanowi inaczej. Wniosek powinien zawierać informacje umożliwiające wyszukanie w zbiorze żądanych danych osobowych oraz wskazywać ich zakres i przeznaczenie.
6. Udostępnione dane osobowe można wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.

Administrator Danych Osobowych lub osoba przez niego upoważniona prowadzi dokument Ewidencji podmiotów, którym Podmiot udostępnia dane osobowe (zał. nr 5). Dokument zawiera informacje o udostępnieniu danych osobowych na rzecz wszystkich podmiotów, z wyłączeniem:

1. osób Upoważnionych do przetwarzania danych osobowych,
2. osób, których dane dotyczą,
3. organów państwowych lub samorządu terytorialnego, którym dane osobowe są udostępniane w związku z prowadzonym postępowaniem.

Zbiór danych

Zbiór danych osobowych to, zgodnie z art. 4 pkt 6 ustawy każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie. Cechą wyróżniającą zbiór danych od innego zestawu danych jest struktura, czyli takie uporządkowanie, które daje możliwość wyszukania konkretnych danych według określonego kryterium.

Każdy zbiór danych osobowych jest opisany oraz zarejestrowany w dokumencie będącym Rejestrem Przetwarzania Danych Osobowych, które przetwarza catering (zał. nr. 9).

Odpowiedzialność karna i dyscyplinarna

1. Wobec osoby, która w przypadku naruszenia zasad bezpieczeństwa lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonych w niniejszej dokumentacji, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, wszczyna się postępowanie dyscyplinarne.
2. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych.
3. Orzeczona kara dyscyplinarna nie wyklucza odpowiedzialności karnej osoby winnej zgodnie z ustawą z dnia 29 sierpnia 1997 roku o ochronie danych osobowych oraz możliwości wytoczenia wobec niej powództwa cywilnego.

V UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Do przetwarzania danych osobowych uprawnione są wyłącznie osoby Upoważnione do przetwarzania danych osobowych
2. Celem niniejszej procedury jest minimalizacja ryzyka nieuprawnionego dostępu do danych osobowych i utraty ich poufności przez osoby nieupoważnione.
3. Administrator Danych Osobowych jest uprawniony do przyznawania upoważnień w przedmiocie przetwarzania danych osobowych, w drodze pisemnego Upoważnienia do przetwarzania danych osobowych (zał. nr 3),
4. Administrator Danych Osobowych może wyznaczyć osoby uprawnione do przyznawania upoważnień w przedmiocie przetwarzania danych osobowych, w drodze pisemnego uprawnienia.
5. Upoważnienie do przetwarzania danych osobowych następuje wyłącznie na podstawie indywidualnego upoważnienia nadanego zgodnie z przepisami ustawy o ochronie danych osobowych oraz RODO.
6. Nadanie upoważnienia do przetwarzania danych osobowych musi nastąpić przed rozpoczęciem przetwarzania danych przez osobę upoważnioną.
7. Administrator Danych Osobowych lub osoba przez niego upoważniona prowadzi dokument Ewidencji osób upoważnionych do przetwarzania danych osobowych (zał. nr 2).
8. W przypadku konieczności nadania bądź zmiany uprawnień (np. z powodu zatrudnienia osoby lub zmiany stanowiska pracy), Administrator Danych Osobowych lub osoba przez niego upoważniona zobowiązany jest do sprawdzenia, czy dana osoba:

    a. odbyła szkolenie z zakresu przestrzegania zasad bezpieczeństwa danych osobowych,
    b. będzie przetwarzała dane osobowe w zakresie i celu określonym w Polityce i instrukcji zarządzania systemem informatycznym.

9. Nadanie upoważnienia do przetwarzania danych osobowych wymaga zaznajomienia się z przepisami dotyczącymi ochrony danych osobowych, w zakresie niezbędnym do czynności wykonywanych w ramach udzielonego upoważnienia.
10. Administrator Danych Osobowych jest odpowiedzialny za organizację i przeprowadzenie szkoleń lub zaznajomienie w innej formie osób upoważnionych z przepisami dotyczącymi ochrony danych osobowych.
11. Odbycie szkolenia z zakresu ochrony danych osobowych zostaje potwierdzone przez osobę w nim uczestniczącą w formie pisemnego Potwierdzenia uczestnictwa w szkoleniu (zał. nr 6).

VI OBOWIĄZKI PODMIOTOWE W OBSZARZE OCHRONY DANYCH OSOBOWYCH

Obowiązki Administratora Danych Osobowych

1. podział zadań i obowiązków związanych z organizacją ochrony danych osobowych,
2. podejmowanie odpowiednich i niezbędnych działań mających na celu zapewnienie prawidłowej ochrony danych osobowych, w szczególności poprzez sporządzanie i wdrażanie właściwych warunków organizacyjnych i technicznych,

3. wprowadzenie do stosowania procedur zapewniających prawidłowe przetwarzanie danych osobowych,
4. egzekwowanie rozwoju środków bezpieczeństwa przetwarzania danych osobowych,
5. poddawanie przeglądom skuteczność Polityki bezpieczeństwa przetwarzania danych osobowych,
6. zapewnianie przestrzegania przepisów o ochronie danych osobowych, w szczególności przez: organizację i nadzorowanie przestrzegania zasad ochrony danych osobowych zarówno w systemach informatycznych, jak również w zbiorach danych osobowych prowadzonych w formie papierowej i elektronicznej,
7. prowadzenie dokumentacji opisującej zastosowaną politykę bezpieczeństwa przetwarzania danych osobowych (niniejsza Polityka oraz wynikające z niej instrukcje i procedury),
8. wdrożenie zapoznania z przepisami dotyczącymi ochrony danych osobowych oraz zagrożeniami związanymi z przetwarzaniem danych przez pracowników Podmiotu,
9. zapewnienie kontroli nad tym, jakie dane osobowe, przez kogo i kiedy zostały wprowadzone do zbioru,
10. nadawanie i uchylanie uprawnień do przetwarzania danych osobowych w cateringu dietetycznym,
11. prowadzenie rejestru osób Upoważnionych do przetwarzania danych, zawierającego imię i nazwisko Upoważnionego, datę nadania i ustania, zakres Upoważnienia do przetwarzania danych osobowych, identyfikator w przypadku gdy Upoważniony został zarejestrowany w systemie informatycznym, służącym do przetwarzania danych osobowych,
12. zapewnienie zapoznania osób Upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych,
13. analiza sytuacji, okoliczności i przyczyn, które doprowadziły do naruszenia ochrony danych osobowych i przygotowanie zaleceń i rekomendacji dotyczących eliminacji ryzyka ich ponownego wystąpienia,
14. prowadzenie zgodnych z Instrukcją działań w przypadku stwierdzenia nieuprawnionego dostępu do bazy danych lub naruszenia zabezpieczenia danych,
15. zapewnienie podstaw prawnych do przetwarzania danych osobowych od chwili zebrania danych osobowych do chwili ich usunięcia,
16. dbałość o prawidłowe przetwarzanie danych osobowych, w szczególności poprzez zapewnienie aktualności, adekwatności oraz merytorycznej poprawności danych osobowych przetwarzanych w określonym przez nich celu,

Obowiązki Upoważnionych

1. znajomość Polityki oraz przepisów powszechnie obowiązującego prawa w obszarze ochrony danych osobowych, przetwarzanych przez catering dietetyczny,
2. znajomość, zrozumienie i stosowanie w możliwie największym zakresie wszelkich dostępnych środków ochrony danych osobowych oraz uniemożliwienie osobom nieuprawnionym dostępu do swojej stacji roboczej,
3. przetwarzanie danych osobowych zgodnie z obowiązującymi przepisami prawa oraz przyjętymi regulacjami, w granicach przyznanego upoważnienia,
4. postępowanie zgodnie z ustalonymi regulacjami wewnętrznymi dotyczącymi przetwarzania danych osobowych,

5. zachowanie w tajemnicy danych osobowych oraz informacji o sposobach ich zabezpieczenia, również po ustaniu zatrudnienia,
6. ochrona danych osobowych oraz środków przetwarzających dane osobowe przed nieuprawnionym dostępem, ujawnieniem, modyfikacją, zniszczeniem lub zniekształceniem,
7. informowanie o wszelkich podejrzeniach naruszenia lub zauważonych naruszeniach oraz słabościach systemu przetwarzającego dane osobowe do przełożonego, który ma obowiązek poinformować Administratora Danych Osobowych.

VII OCENA RYZYKA I PRZEGLĄDY

Uwzględniając kategorie przetwarzanych danych oraz zagrożenia zidentyfikowane w wyniku przeprowadzonej analizy ryzyka, stosuje się wysoki poziom bezpieczeństwa.

1. Przegląd stanu ochrony przetwarzanych przez catering dietetyczny danych jest przeprowadzany przynajmniej raz w roku.
2. Przegląd stanu ochrony przetwarzanych przez catering dietetyczny danych osobowych przeprowadzają Administrator Danych Osobowych lub wyznaczeni kontrolerzy wewnętrzni.
3. Przegląd obejmuje wszystkie obszary działalności i elementy infrastruktury cateringu dietetycznego, w których wymagane jest przestrzeganie zasad przetwarzania danych osobowych, w szczególności systemy informatyczne, zabezpieczenia fizyczne oraz organizacyjne.
4. Kontrolujący przygotowuje plan przeglądu z uwzględnieniem jego zakresu oraz niezbędnych zasobów, takich jak czas i ilość osób dokonujących czynności.
5. Przegląd jest protokołowany.
6. Kontrolujący opracowuje wyniki przeprowadzonego przeglądu, które następnie przekazuje w formie Raportu z przeglądu (zał. nr 7) Administratorowi Danych Osobowych, ewentualnie również kierownikowi kontrolowanej jednostki.
7. Na podstawie raportu pokontrolnego Administrator Danych Osobowych inicjuje działania zapobiegawcze lub kontrolujące.

VIII ZAGROŻENIA BEZPIECZEŃSTWA DANYCH OSOBOWYCH ORAZ INCYDENTY

Na bezpieczeństwo procesu przetwarzania danych osobowych składają się rozliczalność, poufność i integralność przetwarzanych danych. Rozliczalność oznacza możliwość przypisania działań osoby jednoznacznie i wyłącznie tej osobie. Poufność wyraża się zapewnieniem, że przetwarzane dane osobowe nie są udostępniane nieupoważnionym podmiotom. Integralność oznacza zapewnienie niemożliwości zmiany lub nieautoryzowanego zniszczenia danych osobowych.

W przypadku stwierdzenia naruszenia ochrony danych osobowych lub ich zagrożenia, każdy pracownik jest zobowiązany poinformować o tym fakcie Administratora Danych Osobowych, właściwą osobę przez niego upoważnioną lub przełożonego. Osoba upoważniona lub przełożony pracownika jest zobowiązany powiadomić Administratora Danych Osobowych.

Instrukcja postępowania w przypadku zagrożenia bezpieczeństwa danych osobowych

Zagrożeniem bezpieczeństwa informacji jest sytuacja, w której występuje zagrożenie zaistnienia incydentu. Przykładowy katalog zagrożeń:

1. nieprzestrzeganie Polityki przez osoby przetwarzające dane, np. niezamykanie pomieszczeń, szaf, biurek, brak stosowania zasad ochrony haseł,
2. niewłaściwe zabezpieczenie fizyczne dokumentów, urządzeń lub pomieszczeń,
3. niewłaściwe zabezpieczenie oprogramowania lub sprzętu IT przed wyciekiem, kradzieżą lub utratą danych osobowych.

Postępowanie Administratora Danych Osobowych lub osoby przez niego upoważnionej w przypadku stwierdzenia wystąpienia zagrożenia:

1. ustalenie zakresu i przyczyn zagrożenia oraz jego ewentualnych skutków,
2. w miarę możliwości przywrócenie stanu zgodnego z zasadami ochrony danych osobowych,
3. w razie konieczności zainicjowanie działań dyscyplinarnych,
4. zarekomendowanie działań zapobiegawczych w kierunku wyeliminowania podobnych zagrożeń w przyszłości,
5. udokumentowanie prowadzonego postępowania w Rejestrze naruszeń bezpieczeństwa (zał. nr 8).

Instrukcja postępowania w przypadku incydentów bezpieczeństwa danych osobowych

Incydentem jest sytuacja naruszenia bezpieczeństwa informacji ze względu na dostępność, integralność i poufność. Incydenty powinny być wykrywane, rejestrowane i monitorowane w celu zapobieżenia ich ponownemu wystąpieniu. Przykładowy katalog incydentów:

1. losowe zdarzenie wewnętrzne, np. awaria komputera, serwera, twardego dysku, błąd użytkownika, informatyka, zgubienie danych,
2. losowe zdarzenie zewnętrzne, np. klęski żywiołowe, zalanie, awaria zasilania, pożar,
3. incydent umyślny, np. wyciek informacji, ujawnienie danych nieupoważnionym osobom, świadome zniszczenie danych, działanie wirusów komputerowych, włamanie do pomieszczeń lub systemu informatycznego (wewnętrzne i zewnętrzne).

Postępowanie Administratora Danych Osobowych lub właściwej osoby przez niego upoważnionej w przypadku stwierdzenia wystąpienia incydentu:

1. ustalenie czasu zdarzenia będącego incydentem,
2. ustalenie zakresu incydentu,
3. określenie przyczyn, skutków oraz szacowanych zaistniałych szkód,
4. zabezpieczenie dowodów,
5. ustalenie osób odpowiedzialnych za naruszenie,
6. usunięcie skutków incydentu,
7. ograniczenie szkód wywołanych incydentem,
8. zainicjowanie działań dyscyplinarnych,

9. zarekomendowanie działań zapobiegawczych w kierunku wyeliminowania podobnych zagrożeń w przyszłości,
10. udokumentowanie prowadzonego postępowania w Rejestrze naruszeń bezpieczeństwa (zał. nr 8).

Postępowanie Upoważnionego w przypadku stwierdzenia wystąpienia zagrożenia do czasu przybycia Administratora Danych Osobowych lub upoważnionej przez niego osoby:

1. powstrzymanie się od rozpoczęcia lub kontynuowania pracy, jak również od podejmowania jakichkolwiek czynności, mogących spowodować zatarcie śladów naruszenia bądź innych dowodów,
2. zabezpieczenie elementów systemu informatycznego lub kartotek, przede wszystkim poprzez uniemożliwienie dostępu do nich osób nieupoważnionych,
3. podjęcie, stosownie do zaistniałej sytuacji, wszelkich niezbędnych działań celem zapobieżenia dalszym zagrożeniom, które mogą skutkować utratą danych osobowych.

IX WYKAZY

1. **Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane dane osobowe stanowi załącznik nr. 10 do Polityki Bezpieczeństwa Danych Osobowych cateringu dietetycznego**

2. **Rejestr przetwarzania danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych oraz podstaw prawnych stanowi załącznik nr. 11**

Środki organizacyjne

1. Została opracowana i wdrożona polityka bezpieczeństwa;
2. Została opracowana i wdrożona instrukcja zarządzania systemami informatycznymi;
3. Do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające ważne upoważnienia nadane przez administratora danych;
4. Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych;
5. Osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych;
6. Przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego;
7. Osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy;
8. Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane;

9. Przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych;

10. Przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu danych osobowych oraz w warunkach zapewniających bezpieczeństwo danych;
11. Stosuje się pisemne umowy powierzenia przetwarzania danych dla współpracy z podwykonawcami przetwarzającymi dane osobowe;
12. W cateringu dietetycznym prowadzi się politykę czystego biurka i ekranu.

Środki ochrony fizycznej danych

Z komentarzem [P3]: Podaliśmy tutaj kilka przykładów zabezpieczeń fizycznych danych. Jeśli któreś z wymienionych zabezpieczeń Was nie dotyczą, to należy je wykreślić lub dopisać swoje

1. Zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym drzwiami zwykłymi (niewzmacnianymi, nie przeciwpożarowymi).
2. Zbiór danych osobowych przechowywany jest w pomieszczeniu, w którym okna zabezpieczone są za pomocą rolet.
3. Pomieszczenia, w którym przetwarzany jest zbiór danych osobowych wyposażone są w system alarmowy przeciwwłamaniowy.
4. Dostęp do pomieszczeń, w których przetwarzany jest zbiory danych osobowych objęte są systemem kontroli dostępu.
5. Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych kontrolowany jest przez system monitoringu z zastosowaniem kamer przemysłowych.
6. Zbiór danych osobowych w formie papierowej przechowywany jest w niemetalowej szafie.
7. Pomieszczenie, w którym przetwarzane są zbiory danych osobowych zabezpieczone jest przed skutkami pożaru za pomocą systemu przeciwpożarowego i/lub wolnostojącej gaśnicy.
8. Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.

Środki sprzętowe infrastruktury informatycznej i telekomunikacyjnej

1. Zbiór danych osobowych przetwarzany jest przy użyciu komputera przenośnego oraz stacjonarnego.
2. Komputer służący do przetwarzania danych osobowych nie jest połączony z lokalną siecią komputerową.
3. Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
4. Zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity.
5. Użyto system Firewall do ochrony dostępu do sieci komputerowej.
6. Użyto system IDS/IPS do ochrony dostępu do sieci komputerowej.

Środki ochrony w ramach narzędzi programowych i baz danych

1. Zastosowano środki umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego zbioru danych osobowych.

2. Dostęp do zbioru danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
3. Dostęp do zbioru danych osobowych wymaga uwierzytelnienia przy użyciu hasła.
4. Zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego.
5. Wprowadzono zasadę okresowej zmiany haseł do poczty oraz programów służących do przetwarzania danych osobowych co 90.
6. Zastosowano kryptograficzne środki ochrony danych osobowych.
7. Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe.
8. Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.

X POSTANOWIENIA KOŃCOWE

1. Polityka bezpieczeństwa jest dokumentem obowiązującym catering dietetyczny w zakresie wdrażania, przestrzegania i weryfikacji zasad ochrony danych osobowych.
2. Polityka bezpieczeństwa jest dokumentem obowiązującym wszystkie osoby dopuszczone do przetwarzania danych osobowych w ramach działalności cateringu dietetycznego.
3. Każda osoba upoważniona do przetwarzania danych osobowych w ramach działalności cateringu dietetycznego ma obowiązek zapoznania się z niniejszą Polityką bezpieczeństwa.
4. Naruszenie zasad wynikających z Polityki bezpieczeństwa może stanowić podstawę wszczęcia postępowania dyscyplinarnego przeciwko sprawcy naruszenia.
5. Wszczęcie lub przeprowadzenie postępowania dyscyplinarnego przeciwko osobie naruszającej zasady wynikające z Polityki bezpieczeństwa nie wyklucza możliwości wszczęcia postępowania karnego oraz dochodzenia roszczeń z powództwa cywilnego.
6. Polityka bezpieczeństwa wraz z załącznikami wchodzi w życie z dniem jej podpisania przez Administratora Danych Osobowych.
7. W przedmiocie spraw nieuregulowanych Polityką bezpieczeństwa, zastosowanie znajdują przepisy ustawy o ochronie danych osobowych.
8. Załączniki do niniejszej Polityki stanowią jej część pod warunkiem uzupełnienia. Lista załączników:
    - 8.1. Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych (zał. nr 1),
    - 8.2. Ewidencja osób upoważnionych do przetwarzania danych osobowych (zał. nr 2),
    - 8.3. Upoważnienie do przetwarzania danych osobowych (zał. nr 3),
    - 8.4. Ewidencja podmiotów, którym Podmiot powierza dane osobowe (zał. nr 4),
    - 8.5. Ewidencja podmiotów, którym Podmiot udostępnia dane osobowe (zał. Nr 5)
    - 8.6. Potwierdzenie uczestnictwa w szkoleniu (zał. nr 6),
    - 8.7. Raport z przeglądu (zał. nr 7),
    - 8.8. Ewidencja naruszeń bezpieczeństwa (zał. nr 8),
    - 8.9. Wzór umowy powierzenia danych osobowych (zał. 9),
    - 8.10. Wykaz obszaru przetwarzania danych osobowych (zał. 10)
    - 8.11. Rejestr przetwarzania danych osobowych (zał. 11)

Podpis Administratora Danych Osobowych	Data
Tomasz Mazurkiewicz	25 stycznia 2023