00
SPIS TREŚCI DOKUMENTACJI SYSTEMU OCHRONY DANYCH OSOBOWYCH

01
DEKLARACJA STOSOWANIA

Polityka Ochrony Danych Osobowych

w Zakładach Mięsnych Leśniak w Nowym Sączu

Właściciel Zakładów Mięsnych Leśniak deklaruje, że w ramach realizacji usług firmy stosowana jest polityka ochrony danych osobowych, zapewniająca naszym klientom, kontrahentom i pracownikom, bezpieczeństwo i poufność, zwłaszcza w zakresie bezpieczeństwa powierzonych danych osobowych.

Jednocześnie Zakłady Mięsne Leśniak dążą do budowania wizerunku firmy, jako instytucji wiarygodnej, przyjaznej, działającej z literą prawa, którą nasi klienci znają, cenią, mając do niej pełne zaufanie.

Polityka ochrony danych osobowych realizowana jest poprzez:
- Zapewnienie poufności, integralności i dostępności danych osobowych w realizowanych przez Zakłady Mięsne Leśniak usługach.
- Spełnienie wymagań ustawowych w zakresie ochrony danych osobowych.
- Szkolenia i kształtowanie postaw, że za bezpieczeństwo danych osobowych odpowiedzialni są wszyscy pracownicy na swoich stanowiskach pracy i w kontaktach z klientami i instytucjami otoczenia Zakłady Mięsne Leśniak.
- Stosowanie nowoczesnych i bezpiecznych technologii informatycznych.
- Udokumentowany i doskonalony System Ochrony Danych Osobowych.

Wiesław Leśniak
(Właściciel)

02
POLITYKA OCHRONY DANYCH OSOBOWYCH

METRYKA DOKMENTU

Wersja dokumentu	**2.0**
Obowiązuje od:	**20.07.2018**
Zakres zmian w stosunku do poprzedniej wersji:	**Nd.**
Zatwierdził:	**Właściciel Wiesław Leśniak**

SPIS TREŚCI

WSTĘP

Dokumentacja Systemu Ochrony Danych Osobowych jest dokumentem opisującym zasady ochrony danych osobowych stosowane przez Administratora w celu spełnienia wymagań Rozporządzenia PE i RE 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych (RODO).
Polityka stanowi jeden ze środków organizacyjnych, mających na celu wykazanie, że przetwarzanie danych osobowych odbywa się zgodnie z powyższym Rozporządzeniem.

POUCZENIE

Niniejsza dokumentacja ma charakter poufny do użytku wyłącznie wewnątrz organizacji. Nie należy dokumentacji ujawniać lub udostępniać osobom nieupoważnionym. Dokumentacja ta nie stanowi informacji publicznej (w rozumieniu ustawy o dostępie do informacji publicznej). Należy zachować ostrożność w przypadku żądania wglądu do niniejszej dokumentacji przez podmioty kontrolujące. Nie każdy podmiot kontrolujący jest uprawniony do takiego wglądu.

DEFINICJE

Administrator – Zakłady Mięsne Leśniak z siedzibą w Nowym Sączu, 33-300 Nowy Sącz, ul. Axentowicza 20A, numer identyfikacji podatkowej NIP: 734-000-04-51, reprezentowana przez Właściciela Wiesława Leśniaka.
ASI – osoba wyznaczona przez Administratora, pełniąca funkcję Administratora Systemów Informatycznych, odpowiedzialna za realizację zadań związanych z funkcjonowaniem systemów informatycznych, nadzorem nad funkcjonowaniem systemów informatycznych służących do przetwarzania danych osobowych zgodnie z prawem.
ASI – [Łukasz Fikiel /lukasz@zmlesniak.pl, tel. 18 414 00 11]
Dziennik SODO – dokument elektroniczny w postaci Skoroszytu Microsoft EXCEL (plik: 05 Dziennik SODO.xlsx)

1 INWENTARYZACJA DANYCH, ZGODNOŚĆ Z PRAWEM, UPOWAŻNIENIA

1.1 INWENTARTYZACJA DANYCH

1. Dane osobowe wymagające ochrony zostały wykazane w dokumencie 05 Dziennik SODO.
2. Wykaz obejmuje zbiory ze stwierdzonym potencjalnym ryzykiem naruszenia praw lub wolności osób fizycznych.
3. Każdy ze zbiorów jest opisany w sposób umożliwiający przeprowadzenie analizy ryzyka.
4. Opis zbiorów obejmuje takie informacje, jak:
   a. Nazwę zbioru.
   b. Opis celów przetwarzania.
   c. Charakter, zakres, kontekst, dokumentowane dane osobowe.
   d. Odbiorcy.
   e. Funkcjonalny opis operacji przetwarzania.
   f. Aktywa służące do przetwarzania danych osobowych (Informacje, Programy, Systemy operacyjne, Infrastruktura IT, Infrastruktura, Pracownicy i współpracownicy, Outsourcing).
   g. Informacja o konieczności wpisu do rejestru czynności przetwarzania.

1.2 ZGODNOŚĆ Z PRAWEM

1. Administrator zapewnia, że:
   a. Dane są legalnie przetwarzane (na podstawie art. 6,9).
   b. Dane osobowe są adekwatne w stosunku do celów przetwarzania.
   c. Dane osobowe są przetwarzane przez określony konkretny czas (retencja danych).
   d. Wobec osób, które przetwarza Administrator wykonano tzw. obowiązek informacyjny (art. 12, 13 i 14) wraz ze wskazaniem im praw (np. prawa dostępu do danych, przenoszenia, sprostowania, usunięcia, ograniczenia przetwarzania, sprzeciwu).
   e. Zapewniono ochronę danych w przypadku powierzenia przetwarzania danych w postaci umów powierzenia z podmiotami przetwarzającymi (art. 28).
2. Potwierdzenie zgodności z prawem przetwarzanych danych osobowych w zbiorach, znajduje się w dokumencie 05 Dziennik SODO.
3. Klauzule informacyjne znajdują się w załączniku 8.1 Klauzule informacyjne, do niniejszej polityki.

1.3 UPOWAŻNIENIA

1. Administrator odpowiada za nadawanie/anulowanie upoważnień do przetwarzania danych w zbiorach papierowych, systemach informatycznych.
2. Każda osoba upoważniona musi przetwarzać dane wyłącznie na polecenie administratora lub na podstawie przepisu prawa.
3. Upoważnienia nadawane są do zbiorów na wniosek przełożonych osób zgodnie ze wzorem wskazanym w załączniku 8.2 Wzór upoważnienia do przetwarzania danych osobowych, do niniejszej polityki.
4. Upoważnienia mogą być nadawane w formie poleceń, np. upoważnienia do przeprowadzenia kontroli, audytów, wykonania czynności służbowych, udokumentowanego polecenia administratora lub w postaci umowy powierzenia.
5. Administrator prowadzi ewidencję osób upoważnionych w celu sprawowania kontroli nad prawidłowym dostępem do danych osób upoważnionych. Ewidencja ma charakter pomocniczy. Wzór ewidencji zawarty jest w dokumencie 05 Dziennik SODO.

2 PROCEDURA ANALIZY RYZYKA / OCENA SKUTKÓW

1. Procedura opisuje sposób przeprowadzenia analizy ryzyka w celu zabezpieczenia danych osobowych adekwatnie do zidentyfikowanych zagrożeń.
2. Przyjęto, że analiza ryzyka przeprowadzana jest dla zbioru danych osobowych lub grupy zbiorów charakteryzujących się podobieństwem celów i sposobów przetwarzania.
3. W przypadku konieczności przeprowadzenia oceny skutków (Art. 35), Administrator przeprowadza ocenę skutków za pomocą narzędzia „CNIL PIA software" dostępnego pod adresem: https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment
4. Celem analizy ryzyka jest zastosowanie środków technicznych i organizacyjnych zapewniających stopień bezpieczeństwa odpowiadający ryzyku wynikającemu z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.
5. Definicje:
   a. Aktywa – środki materialne i niematerialne mające wpływ na przetwarzanie danych osobowych.
   b. Naruszenie (Incydent) ochrony danych osobowych - to naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
   c. Zagrożenie - potencjalne naruszenie (potencjalny incydent).
   d. Skutki - rezultaty niepożądanego incydentu (straty w wypadku wystąpienia zagrożenia).
   e. Ryzyko - prawdopodobieństwo, że określone zagrożenie wystąpi i spowoduje straty lub zniszczenie zasobów.
6. Wyznaczenie zbiorów do analizy ryzyka z aktywami
   a. Analizie ryzyka poddawane są zbiory danych osobowych lub procesy przetwarzania, np. Zbiór pracowników, Zbiór Klientów, Proces obsługi korespondencji.
   b. Do analizy wymagane jest zidentyfikowanie aktywów.
   c. Wykaz przykładowych aktywów znajduje się w dokumencie 06 Analiza Ryzyka – Przykłady.
7. Wyznaczenie zagrożeń
   a. Administrator z ewentualnym współudziałem IOD jest odpowiedzialny za określenie listy możliwych zagrożeń, które mogą wystąpić w przetwarzaniu danych w zbiorze lub w procesie przetwarzania.
   b. Zagrożenia powinny być identyfikowane w odniesieniu do aktywów.
   c. Wykaz przykładowych zagrożeń znajduje się w dokumencie 06 Analiza Ryzyka – Przykłady.
8. Wyliczenie ryzyka dla zagrożeń
   a. Administrator przeprowadza analizę ryzyka za pomocą arkusza Analizy zawartego w dokumencie 05 Dziennik SODO.
   b. Administrator określa Prawdopodobieństwo (P) wystąpienia poszczególnych zagrożeń w zbiorze lub w procesie przetwarzania.
   c. Proponowaną skalę prawdopodobieństwa prezentuje Tabela A.
   d. Administrator określa Skutki (S) wystąpienia incydentów (materializacji zagrożeń), uwzględniając straty finansowe, utratę reputacji, sankcje/skutki karne.
   e. Proponowaną Skalę skutków prezentuje Tabela B.
   f. Administrator wylicza Ryzyka (R) dla wszystkich zagrożeń i ich skutków w/g formuły: R=P*S

Tabela A PRAWDOPODOBIEŃSTWO WYSTĄPIENIA ZAGROŻENIA	SKALA (WAGA)
zagrożenie niskie	**1**
zagrożenie średnie	**2**
zagrożenie wysokie	**3**

Tabela B SKUTKI WYSTĄPIENIA ZAGROŻENIA	SKALA (WAGA)
małe (do 10 000 PLN, incydent prasowy lokalny)	**1**
średnie (10 000 – 100 000 PLN, incydent prasowy ogólnopolski)	**2**
duże (od 100 000 PLN, naruszenie prawa)	**3**

9. Porównanie wyliczonych ryzyk ze skalą i określenie dalszego postępowania z ryzykiem
   a. Administrator porównuje wyliczone ryzyka ze skalą i podejmuje decyzje dotyczące dalszego postępowania z ryzykiem.
   b. Proponowaną skalę Ryzyka prezentuje Tabela C.

Tabela C POZIOM RYZYKA	WARTOŚĆ [R=P*S]
ryzyko pomijalne i akceptowalne (akceptujemy)	**1-2**
ryzyko jest opcjonalne (akceptujemy albo obniżamy)	**3-6**
ryzyko jest nieakceptowalne (musimy obniżyć)	**9**

10. Reakcja na wartość ryzyka
    a. Akceptacja ryzyka – zabezpieczenia są właściwe – brak potrzeby stosowania dodatkowych zabezpieczeń.
    b. Działania obniżające ryzyko, które może zastosować Administrator:
       - Przeniesienie – przerzucenie ryzyka (outsourcing, ubezpieczenie).
       - Unikanie – eliminacja działań powodujących ryzyko (np. zakaz wynoszenia komputerów przenośnych poza obszar organizacji).
       - Redukcja – zastosowanie zabezpieczeń w celu obniżenia ryzyka (np. zaszyfrowanie pendrivów z danymi wynoszonych poza firmę).
    c. Wykaz przykładowych zabezpieczeń znajduje się w dokumencie 06 Analiza Ryzyka.
11. Plan postępowania z ryzykiem
    a. Wszędzie, gdzie Administrator decyduje się obniżyć ryzyko, wyznacza listę zabezpieczeń do wdrożenia, termin realizacji i osoby odpowiedzialne.
    b. Administrator zobowiązany jest do monitorowania wdrożenia zabezpieczeń.
12. Ponowna analiza ryzyka
    a. Ponowna analiza ryzyka przeprowadzana jest cyklicznie lub po znaczących zmianach w przetwarzaniu danych (np. przetwarzanie nowych zbiorów, nowych procesów przetwarzania, zmiany prawne).
    b. W przypadku, gdy analiza ryzyka prowadzona jest w ramach Oceny skutków, wymagana jest do przeprowadzenia przynajmniej raz na 3 lata.
13. Narzędzie do przeprowadzenia analizy ryzyka
    a. Analizę ryzyka przeprowadza się w specjalnym szablonie w dokumencie 05 Dziennik SODO.

3 INSTRUKCJA POSTĘPOWANIA Z INCYDENTEM

Procedura definiuje katalog podatności i incydentów zagrażających bezpieczeństwu danych osobowych oraz opisuje sposób reagowania na nie. Jej celem jest minimalizacja skutków wystąpienia incydentów bezpieczeństwa oraz ograniczenie ryzyka powstania zagrożeń i występowania incydentów w przyszłości.

1. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do powiadamiania o stwierdzeniu podatności lub wystąpieniu incydentu, bezpośredniego przełożonego (lub jeśli jest powołany – Inspektora Ochrony Danych).
2. Do typowych podatności bezpieczeństwa danych osobowych należą:
   a. niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów
   b. niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych
   c. nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka / ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek).
3. Do typowych incydentów bezpieczeństwa danych osobowych należą:
   a. zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności)
   b. zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata / zagubienie danych)
   c. umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania).
4. W przypadku stwierdzenia wystąpienia incydentu, Administrator (lub w przypadku powołania – IOD) prowadzi postępowanie wyjaśniające w toku, którego:
   a. ustala zakres i przyczyny incydentu oraz jego ewentualne skutki
   b. inicjuje ewentualne działania dyscyplinarne
   c. działa na rzecz przywrócenia działań organizacji po wystąpieniu incydentu
   d. rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych incydentów w przyszłości lub zmniejszenia strat w momencie ich zaistnienia.
   e. Administrator dokumentuje powyższe wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze w dokumencie 05 Dziennik SODO.
5. Zabrania się świadomego lub nieumyślnego wywoływania incydentów przez osoby upoważnione do przetwarzania danych.
6. W przypadku naruszenia ochrony danych osobowych skutkującego ryzykiem naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu.

4 REGULAMIN OCHRONY DANYCH OSOBOWYCH

1. Regulamin ma na celu zapewnienie wiedzy osobom przetwarzającym dane osobowe odnośnie bezpiecznych zasad przetwarzania. Zawarty jest w dokumencie 03 Regulamin ODO.
2. Po zapoznaniu się z zasadami ochrony danych osobowych, osoby zobowiązane są do potwierdzenia znajomości tych zasad i deklaracji ich stosowania w załączniku 8.3 Wzór oświadczenia o zachowaniu poufności.

5 SZKOLENIA

1. Każda osoba przed dopuszczeniem do pracy z danymi osobowymi winna być poddana przeszkoleniu i zapoznana z przepisami RODO oraz typowymi zagrożeniami przy przetwarzaniu danych.
2. Za przeprowadzenie szkolenia odpowiada Administrator.

3. Szkolenie prowadzone jest w formie szkolenia e-learningowego (jednorazowo). Szkolenia powtarzane będą raz w roku w formie stacjonarnej (papierowej).
4. Dokumentację szkolenia stanowi program szkolenia oraz lista obecności w wersji papierowej.

6 REJESTR CZYNNOŚCI PRZETWARZANIA I KATEGORII CZYNNOŚCI PRZETWARZANIA

1. W przypadku konieczności prowadzenia rejestru czynności przetwarzania przez Administratora, wypełnia on odpowiednią tabelę w dokumencie 05 Dziennik SODO.
2. W przypadku konieczności prowadzenia rejestru kategorii czynności przetwarzania przez Administratora, wypełnia on odpowiednią tabelę w dokumencie 05 Dziennik SODO.

7 AUDTY

1. Zgodnie z art. 32 RODO, Administrator powinien regularnie testować, mierzyć i oceniać skuteczność środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.
2. Celem audytów wewnętrznych jest ocena, czy system ochrony danych osobowych jest skutecznie wdrożony i funkcjonuje zgodnie z wymaganiami RODO. Audyty prowadzone są w sposób obiektywny i bezstronny. Przestrzegana jest zasada, że audytorzy nie audytują własnej pracy.
3. Administrator jest odpowiedzialny za planowanie i przeprowadzanie audytów wewnętrznych z roczną częstotliwością lub częściej.
4. Administrator opracowuje programy audytów biorąc pod uwagę ważność procesów przetwarzania oraz audytowanych obszarów, jak też wyniki wcześniejszych audytów. Określa on kryteria audytu, jego cel, zakres i ewentualnie metody.
5. Administrator wyznacza audytora do przeprowadzenia audytu.
6. Audytor jest zobowiązany do przygotowania się do przeprowadzenia audytu, zapoznając się z opisem audytowanego obszaru, stosowanych procedur i wyników poprzednich audytów.
7. Audytor realizuje działania audytowe mające na celu uzyskanie obiektywnych dowodów potwierdzających poprawność realizowanych zadań, procedur, polityk, zabezpieczeń, celów, spełniania wymagań RODO.
8. W przypadku stwierdzenia uchybień mających wpływ na skuteczność działania systemu ochrony danych zgodnego z RODO, audytor identyfikuje tzw. uchybienia lub spostrzeżenia
9. Wynik audytu zostaje udokumentowany przez audytora i przekazany Administratorowi. Administrator (ewentualnie IOD) dokonuje przeglądu i analizy wyniku audytu oraz decyduje o inicjowaniu działań korygujących, w przypadku zaistnienia poważnych uchybień.

8 ZAŁĄCZNIKI

8.1 ZAŁĄCZNIK. KLAUZULE INFORMACYJNE (WZORCOWE)

Informacje podawane w przypadku zbierania danych od osoby, której dane dotyczą

Zgodnie z art. 13 ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016r. informuję, iż:

1) Administratorem Pani/Pana danych osobowych jest firma Zakłady Mięsne Leśniak z siedzibą w Nowym Sączu, 33-300 Nowy Sącz, ul. Axentowicza 20A, numer identyfikacji podatkowej NIP:734-000-04-51.
2) Pani/Pana dane osobowe przetwarzane będą w celu zatrudnienia oraz realizacji usług związanych z przedmiotem działalności na podstawie Art. 6 ust. 1 lit. a, b, c, d, e, f lub Art. 9 ust. 1 lit. a, b, c, d, h, i, j ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r.
3) Odbiorcami Pani/Pana danych osobowych będzie Administrator oraz osoba przez niego upoważniona.
4) Pani/Pana dane osobowe przechowywane będą przez okres wskazany w odrębnych ustawach, właściwy dla danego rodzaju dokumentów.
5) Posiada Pani/Pan prawo do: żądania od Administratora dostępu do danych osobowych, prawo do ich sprostowania, usunięcia lub ograniczenia przetwarzania, prawo do wniesienia sprzeciwu wobec przetwarzania, a także prawo do przenoszenia danych.
6) Ma Pani/Pan prawo wniesienia skargi do UODO, gdy uzasadnione jest, że Pani/Pana dane osobowe przetwarzane są przez Administratora niezgodnie z ogólnym rozporządzeniem o ochronie danych osobowych z dnia 27 kwietnia 2016r.
7) Podanie danych osobowych jest dobrowolne/obligatoryjne na mocy przepisu prawa, jednakże niepodanie danych w zakresie wymaganym przez Administratora może skutkować **niemożnością realizacji celu przetwarzania.**

Informacje podawane w przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą:

Zgodnie z art. 14 ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016r. informuję, iż:

1) Administratorem Pani/Pana danych osobowych jest firma Zakłady Mięsne Leśniak z siedzibą w Nowym Sączu, 33-300 Nowy Sącz, ul. Axentowicza 20A, numer identyfikacji podatkowej NIP:734-000-04-51.
2) Pani/Pana dane osobowe przetwarzane będą w celu zatrudnienia oraz realizacji usług związanych z przedmiotem działalności na podstawie Art. 6 ust. 1 lit. a, b, c, d, e, f lub Art. 9 ust. 1 lit. a, b, c, d, h, i, j ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r.
3) Kategoria danych osobowych: dane osobowe zwykłe/dane osobowe szczególnie chronione*
4) Pani/Pana dane osobowe pozyskano ze źródeł publicznie dostępnych.
5) Odbiorcami Pani/Pana danych osobowych będzie Administrator oraz osoba przez niego upoważniona.
6) Pani/Pana dane osobowe przechowywane będą przez okres wskazany w odrębnych ustawach, właściwy dla danego rodzaju dokumentów.
7) Ma Pani/Pan prawo wniesienia skargi do UODO, gdy uzasadnione jest, że Pani/Pana dane osobowe przetwarzane są przez Administratora niezgodnie z ogólnym rozporządzeniem o ochronie danych osobowych z dnia 27 kwietnia 2016r.

8) Podanie danych osobowych jest dobrowolne/obligatoryjne na mocy przepisu prawa, jednakże niepodanie danych w zakresie wymaganym przez Administratora może skutkować **niemożnością realizacji celu przetwarzania.**

Opcjonalnie do zastosowani w obu klauzulach:

1) Informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu.
2) Informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem.
3) Jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f) – prawnie uzasadnione interesy realizowane przez administratora lub przez stronę trzecią.
4) Informacje o zamiarze przekazania danych osobowych odbiorcy w państwie trzecim lub organizacji międzynarodowej.

Materiał pomocniczy art. 13 i 14 RODO.

8.2 ZAŁĄCZNIK. WZÓR UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH

UPOWAŻNIENIE
do przetwarzania danych osobowych
w systemach informatycznych lub zbiorach w wersji papierowej

Z dniem ……. upoważniam Panią / Pana * ……
Zatrudnioną / zatrudnionego na stanowisku ……..

do przetwarzania danych osobowych zawartych w zbiorach danych osobowych prowadzonych przez Administratora (lub powierzonych Administratorowi do przetwarzania), w postaci papierowej i/lub elektronicznej, zgodnie z przydzielonym zakresem obowiązków.
Przetwarzanie jest dopuszczalne za pomocą systemów przetwarzania do których otrzymał/otrzymała Pani/Pan dostęp. Zakres wykonywanych przez Panią/Pana operacji na danych osobowych wynika z zakresu obowiązków i/lub poleceń wydanych przez Administratora.

Upoważnienie jest ważne od dnia ……. **na czas nieokreślony**.
Wszystkie wcześniej wydane upoważnienia do przetwarzania danych osobowych tracą moc i zostają anulowane.

Nowy Sącz, ……..
(miejscowość i data)

……
(pieczęć i podpis Administratora)

……
Potwierdzam odbiór upoważnienia:
(podpis pracownika)

Podstawa prawna:

Art. 29 i 32 ust. 4 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE… (Dz. Urz. UE L 119/1 z 4.5.2016 r.).

Anulowanie upoważnienia

Z dniem …….. anuluję niniejsze upoważnienie.

Nowy Sącz, ……
(miejscowość i data)

(pieczęć i podpis Administratora)

8.3 ZAŁĄCZNIK. WZÓR OŚWIADCZENIA O ZACHOWANIU POUFNOŚCI

…….. ……..
(imię i nazwisko) (miejscowość i data)

OŚWIADCZENIE O POUFNOŚCI

Oświadczam, iż zapoznano mnie z przepisami dotyczącymi ochrony danych osobowych, w szczególności Rozporządzenia Parlamentu Europejskiego Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. 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) zwanego dalej „RODO", Ustawy o Ochronie Danych Osobowych z dnia 10 maja 2018r. Dz.U. 2018 poz. 1000) oraz odnośnymi wymaganiami wewnętrznego „Regulaminu Ochrony Danych Osobowych".

W szczególności zobowiązuje się do:

- przetwarzania danych osobowych wyłącznie w zakresie i celu przewidzianym w powierzonych przez Administratora zadaniach,
- zachowania w tajemnicy danych osobowych do których mam lub będę miał/a dostęp w związku z wykonywaniem zadań powierzonych przez Administratora,
- niewykorzystywania danych osobowych w celach niezgodnych z zakresem i celem powierzonych zadań przez Administratora,
- zachowania w tajemnicy sposobów zabezpieczenia danych osobowych
- ochrony danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją danych osobowych, nieuprawnionym ujawnieniem danych osobowych, nieuprawnionym dostępem do danych osobowych oraz przetwarzaniem.

Przyjmuję do wiadomości, iż powyższe zasady przetwarzania obowiązują mnie w trakcie trwania stosunku pracy / umowy / stażu / praktyki *, a także po jego/jej zakończeniu – bezterminowo.

Przyjmuję do wiadomości, iż postępowanie sprzeczne z powyższymi zobowiązaniami, może być uznane przez Pracodawcę za ciężkie naruszenie obowiązków pracowniczych w rozumieniu art. 52 § 1 pkt 1 Kodeksu Pracy, naruszenie przepisów Ustawy o Ochronie Danych Osobowych, a także Rozporządzenia o Ochronie Danych UE z dnia 27 kwietnia 2016r.

Odpowiedzialności karnej podlegają konkretne osoby fizyczne, którym ta odpowiedzialność może zostać przypisana, według zasad przewidzianych w prawie karnym materialnym i procesowym.

Jestem świadomy w razie naruszenia dobra osobistego osoby, której dane są przetwarzane, sąd może przyznać temu, czyje dobro osobiste zostało naruszone, odpowiednią sumę tytułem zadośćuczynienia pieniężnego za doznaną krzywdę.

* niepotrzebne skreślić

……
(podpis oświadczającego)

8.4 ZAŁĄCZNIK. WZÓR UMOWY POWIERZENIA DANYCH DO PRZETWARZANIA

UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

zawarta w …….. w dniu ……..r. pomiędzy:

Firmą Zakłady Mięsne Leśniak z siedzibą w Nowym Sączu, 33-300 Nowy Sącz, ul. Axentowicza 20A, numer identyfikacji podatkowej NIP: 734-000-04-51, reprezentowanym przez: Wiesława Leśniaka – Prezesa, zwanego dalej **Zleceniodawcą**

a

[firma] z siedzibą w [adres], NIP […], REGON […], KRS […], reprezentowaną przez: [imię, nazwisko] – [funkcja], zwanego dalej **Zleceniobiorcą**

o treści następującej

1. Przetwarzanie danych osobowych z tytułu Umowy odbywać się będzie w zgodzie i w oparciu o: Rozporządzenie Parlamentu Europejskiego 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) zwanego dalej „RODO“, Ustawę o Ochronie Danych Osobowych z dnia 10 maja 2018r. (Dz.U. 2018 poz. 1000).
2. Administratorem danych osobowych, których przetwarzanie wynika z Umowy jest Zleceniodawca.
3. Podmiotem przetwarzającym, któremu Zleceniodawca powierza przetwarzanie danych osobowych jest Zleceniobiorca.
4. Okres obowiązywania umowy wynika bezpośrednio z zawartej Umowy i jest równy okresowi na jaki została zawarta Umowa.
5. Cel i zakres powierzenia przetwarzania danych osobowych wynika bezpośrednio i ogranicza się wyłącznie do zadań/czynności wynikających z zawartej Umowy. tj.: Świadczenia usługi zgodnie z Umową.
   a. Kategorie przetwarzanych danych: [pracownicy, kontrahenci, klienci, kandydaci do pracy, zapisy monitoringi video]
   b. Rodzaj przetwarzanych danych: [imię, nazwisko, numer pesel, data urodzenia, adres zamieszkania, numer telefonu, adres e-mail, dane identyfikacyjne dotyczące dostawców i odbiorców, itp.]
   c. Miejsce przetwarzania: [w siedzibie Administratora: Nowy Sącz, ul. Axentowicza 20A]
   d. Na powyższych danych będą wykonywane w szczególności operacje: [wgląd, wprowadzanie do rejestrów, dokumentacji i systemów księgowych i informatycznych, nanoszenie zmian, itp.].

6. Zleceniobiorca zobligowany jest szczególnie do:
   a. Zapewnienia bezpiecznego (kryptograficznie zabezpieczonego) transferu danych w procesie świadczonych usług związanych ze zdalnym dostępem;
   b. Wdrożenia mechanizmów uwierzytelniania oraz nadzoru działań w systemie przez odnotowywanie zdarzeń (logowanie działań),
   c. Zapewnienia w działaniach serwisowych by dostęp do zasobów był ograniczony do osób upoważnionych.

7. Przetwarzanie danych osobowych przez Zleceniobiorcę będzie odbywać się wyłącznie na polecenie Zleceniodawcy.

8. Do przetwarzania danych osobowych ze strony Zleceniobiorcy mogą być dopuszczone wyłącznie osoby posiadające upoważnienie, o których mowa w art. 29 RODO oraz przeszkolone z zakresu przepisów dotyczących ochrony danych osobowych.

9. Zleceniodawca upoważnia Zleceniobiorcę do wyznaczania osób uprawnionych do przetwarzania danych osobowych w zakresie koniecznym do wypełnienia zobowiązania z tytułu realizowania zapisów niniejszej umowy.

10. Zleceniobiorca oświadcza, że każda osoba (np. pracownik etatowy, osoba świadcząca czynności na podstawie umów cywilnoprawnych oraz inne osoby pracujące na rzecz Zleceniobiorcy), która zostanie upoważniona do przetwarzania danych osobowych będących przedmiotem Umowy, zostanie zobowiązana do zachowania tych danych w tajemnicy przed udostępnieniem jej ww. danych. Tajemnica ta obejmuje również wszelkie informacje dotyczące sposobów zabezpieczenia powierzonych do przetwarzania danych osobowych.

11. Zleceniobiorca realizując zadania wynikające z Umowy:
   a. Zastosuje środki zabezpieczenia określone w art. 32 RODO najpóźniej z dniem 25 maja 2018r., przy czym wdrożone środki zabezpieczenia muszą być adekwatne do zidentyfikowanych ryzyk dla zakresu powierzonego przetwarzania danych.
   b. Udzieli pomocy Zleceniodawcy w zakresie:
      i. realizacji obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III RODO,
      ii. zapewnienia realizacji obowiązków wynikających z art. 32–36 RODO,
      iii. bezzwłocznie - nie później jednak niż w ciągu 48 godzin od jego wykrycia – zgłosi Zleceniodawcy każde naruszenie danych osobowych, którego będzie uczestnikiem,
   c. po zakończeniu przetwarzania danych osobowych niezwłocznie zwróci powierzone mu dane lub dokona ich zniszczenia – adekwatnie do woli Zleceniodawcy,
   d. udostępni Zleceniodawcy wszelkie informacje niezbędne do wykazania spełnienia obowiązków spoczywających na Podmiocie Przetwarzającym oraz umożliwi Zleceniodawcy lub audytorowi upoważnionemu przez Zleceniodawcę przeprowadzanie audytów, w tym inspekcji, współpracując przy działaniach sprawdzających i naprawczych,
   e. zastosuje się do zaleceń pokontrolnych przekazanych przez Zleceniodawcę,
   f. rozpocznie prowadzenie rejestru wszystkich kategorii czynności przetwarzania dokonywanych w imieniu Administratora zgodnie z wymaganiami art. 30 ust 2 RODO najpóźniej w dniu 25.05.2018r.
   g. wyznaczył u siebie Inspektora Ochrony Danych zgodnie z wymaganiami art. 37 ust 2 RODO

12. Zleceniodawca wyraża ogólną zgodę na to, by Zleceniobiorca realizując zadania określone w Umowie korzystał z usług innego podmiotu przetwarzającego, przy czym:
   a. Zleceniobiorca zobowiązany jest poinformować pisemnie Zleceniodawcę o wszelkich zamierzonych działaniach dotyczących dodania, zmianach lub zastąpienia innych podmiotów przetwarzających, dając tym samym Administratorowi danych osobowych możliwość wyrażenia sprzeciwu wobec tych działań.
   b. Podpowierzenie przetwarzania przez Zleceniobiorcę podmiotowi przetwarzającemu wymaga formy umowy pisemnej lub zastosowania standardowych klauzul umownych w przypadku,

kiedy stroną jest podmiot przetwarzający dane w państwie trzecim. Zawarta umowa musi zawierać wszystkie zobowiązania określone w niniejszej umowie oraz precyzować: czas, charakter i cel przetwarzania danych z uwzględnieniem zakresu (lub kategorii) przetwarzanych danych.

c. Zleceniobiorca odpowiada za działania podmiotu przetwarzającego jak za własne.

13. Zleceniobiorca odpowiada za szkody poniesione przez właściciela danych oraz Zlecającego z tytułu działań niezgodnych z zapisami niniejszej umowy oraz RODO.

WYKONAWCA **ZLECAJĄCY**

8.5 ZAŁĄCZNIK. WZÓR FORMULARZA ZGODY NA WYKORZYSTANIE DANYCH BIOMETRYCZNYCH (ZAMEK ELEKTRONICZNY DO DRZWI OTWIERANYCH NA PALEC) - NIE DOTYCZY

Zgoda na przetwarzanie danych biometrycznych (odwzorowania cyfrowego linii papilarnych)

Imię: ……

Nazwisko: ……

PESEL: ……

☐ Niniejszym wyrażam zgodę na przetwarzanie moich danych biometrycznych (odwzorowania cyfrowego linii papilarnych) wyłącznie w celu ułatwienia wejścia na teren siedziby Zakładów Mięsnych Leśniak.

☐ Nie wyrażam zgody a przetwarzanie moich danych biometrycznych (odwzorowania cyfrowego linii papilarnych). Proszę o wydanie karty zbliżeniowej w celu wejścia na teren siedziby Zakładów Mięsnych Leśniak.

Oświadczam, że zostałem poinformowany iż:

1. Administratorem moich danych osobowych jest Firma Zakłady Mięsne Leśniak z siedzibą w Nowym Sączu, 33-300 Nowy Sączu, ul. Axentowicza 20A, numer identyfikacji podatkowej NIP: 734-000-04-51. Moje dane będą przetwarzane wyłącznie w celu wejścia do budynku siedziby Zakładów Mięsnych Leśniak.
2. Dane są przetwarzane na podstawie art. 6 ust.1 lit. a (wyrażenie zgody) ogólnego rozporządzenia o ochronie danych osobowych UE.
3. Moje dane biometryczne będą wykorzystane wyłącznie w celu dostępu do budynku, nie będą wykorzystywane do rejestracji czasu pracy i monitorowania lokalizacji.
4. Moje dane biometryczne nie będą powierzane i udostępniane.
5. Dane biometryczne przechowywane będą do momentu odwołania zgody lub ustania stosunku pracy.
6. Posiadam prawo do: żądania od administratora dostępu do danych osobowych, prawo do ich sprostowania, usunięcia lub ograniczenia przetwarzania, prawo do wniesienia sprzeciwu wobec przetwarzania, a także prawo do przenoszenia danych.
7. Mam prawo wniesienia skargi do UODO, gdy uzasadnione jest, że Pana/Pani dane osobowe przetwarzane są przez administratora niezgodnie z ogólnym rozporządzeniem o ochronie danych osobowych z dnia 27 kwietnia 2016 r.
8. Podanie danych biometrycznych jest dobrowolne, jednakże niepodanie danych skutkować będzie brakiem możliwości korzystania z ułatwienia wejścia i koniecznością stosowania karty lub wejścia na „żądanie".

Data: …… Czytelny podpis pracownika ……..

8.6 ZAŁĄCZNIK. WZÓR OBOWIĄZKU INFORMACYJNEGO DO UMIESZCZENIA NA STRONIE INTERNETOWEJ

Ochrona danych osobowych – wypełnienie obowiązku informacyjnego.

Administratorem danych osobowych (dalej Administrator) jest Zakłady Mięsne Leśniak z siedzibą w Nowym Sączu, 33-300 Nowy Sącz, ul. Axentowicza 20A, numer identyfikacji podatkowej NIP: 734-000-04-51.

W jakim celu przetwarzamy dane osobowe:

- w celu podjęcia działań przed zawarciem umowy oraz w celu zawarcia i realizacji umowy,
- w celach informacyjnych i marketingowych, wyłącznie na podstawie zgody zgodnie z treścią udzielonej zgody,
- w celu ochrony przed zagrożeniami zewnętrznymi oraz wewnętrznymi (zwiększenie bezpieczeństwa pracowników oraz bezpieczeństwa technologicznego),
- w celu zatrudniania pracowników i prowadzenia procesów rekrutacji.

Jak długo przetwarzamy dane osobowe:

W zależności od celu przetwarzania dane osobowe będą przechowywane

- *przez okres trwania umowy oraz po zakończeniu jej trwania w celu wypełnienia obowiązku prawnego ciążącego na Administratorze,*
- *na czas zgodny z obowiązującymi przepisami prawa*
- *w przypadku prawnie usprawiedliwionych celów Administratora, w tym sprzedaży i marketingu bezpośredniego, do czasu cofnięcia przez osobę której dane dotyczą zgody.*
- *W przypadku monitoringi wideo (CCTV) przez okres do* 21 *dni.*

Komu powierzamy i udostępniamy dane osobowe:

Pozyskanych danych osobowych nie udostępniamy i nie przekazujemy innym podmiotom. W szczególnych przypadkach (wykroczenia lub przestępstwa) dane mogą być udostępnione organom ścigania. Dane mogą być także udostępniane organom Państwa wyłącznie na podstawie przepisów prawa.

Dane osobowe możemy powierzyć do przetwarzania w naszym imieniu podmiotom realizującym dla nas usługi wspierające np. podwykonawstwo, hostowane strony internetowej, wysyłka newslettera, świadczenie usług księgowych, obsługa serwisowa naszych systemów informatycznych. W takim przypadku nadal jesteśmy Administratorem danych i odpowiadamy za przetwarzanie danych .

Prawa które przysługują osobie której dane przetwarzamy:

Osoba fizyczna ma prawo dostępu do treści swoich danych osobowych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przenoszenia danych, prawo do wniesienia sprzeciwu, prawo do cofnięcia zgody w dowolnym momencie.

Osoba fizyczna ma prawo wniesienia skargi do Urzędu Ochrony Danych Osobowych, gdy uzna, że przetwarzanie jej danych osobowych narusza przepisy rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 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) (Dz. Urz. UE L 119 z 4.05.2016).

8.7 ZAŁĄCZNIK. WZÓR KLAUZULI INFORMACYJNEJ

Wzór klauzuli informacyjnej do faktur (skrócona klauzula do umieszczenia w stopce faktury)

Informujemy, że Administratorem Państwa danych osobowych jest Firma Zakłady Mięsne Leśniak z siedzibą w Nowym Sączu, 33-300 Nowy Sącz, ul. Axentowicza 20A, numer identyfikacji podatkowej NIP: 734-000-04-51. Szczegółowe informacje o zasadach przetwarzania danych osobowych przez Zakłady Mięsne Leśniak dostępne są na naszej stronie internetowej www.zmlesniak.pl

Wzór skróconej klauzuli informacyjnej dla odbiorców, klientów zewnętrznych

ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

Administratorem Państwa danych osobowych jest Firma Zakłady Mięsne Leśniak z siedzibą w Nowym Sączu, 33-300 Nowy Sącz, ul. Axentowicza 20A, numer identyfikacji podatkowej NIP: 734-000-04-51. Szczegółowe informacje dotyczące przetwarzania danych osobowych dostępne są na stronie internetowej Zakładów Mięsnych Leśniak pod adresem: www.zmlesniak.pl oraz w siedzibie Administratora.

Wzór pełnej klauzuli informacyjnej dla odbiorców, klientów zewnętrznych

ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

Firma Zakłady Mięsne Leśniak przetwarza Państwa dane osobowe wyłącznie w celu realizacji usług związanych z przedmiotem działalności. W związku z powyższym zgodnie z art. 13 ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016r. informujemy:

1. Administratorem danych osobowych jest Firma Zakłady Mięsne Leśniak z siedzibą w Nowym Sączu, 33-300 Nowy Sącz, ul. Axentowicza 20A, numer identyfikacji podatkowej NIP: 734-000-04-51.
2. Państwa dane osobowe przetwarzane będą na podstawie przepisów prawa w zakresie i celu niezbędnym do realizacji umów, rozpatrywania wniosków, przyjmowana deklaracji, rozliczania, wykonywania kontroli, windykacji należności, innych obowiązków prawnych ciążących na Zakładach Mięsnych Leśniak, a także podjęcia przez Zakłady Mięsne Leśniak działań przed zawarciem umowy lub w celu dochodzenia lub obrony przed roszczeniami.
3. Państwa Dane mogą być powierzane podmiotom współpracującym z nami wyłącznie w celu realizacji wyżej wskazanych usług lub spełnienia obowiązku prawa np. operatorom pocztowym, firmom kurierskim, podmiotom świadczącym na rzecz Zakładów Mięsnych Leśniak usługi doradcze, podmiotom zapewniającym obsługę informatyczną oraz archiwom. W takim przypadku nadal jesteśmy Administratorem tych danych i odpowiadamy za ich przetwarzanie.
4. Dane mogą być udostępniane innym podmiotom w celu windykacji należności i dochodzenia praw Administratora.
5. Państwa dane będą przechowywane przez okres wymagany przepisami prawa, na podstawie których Państwa dane są przetwarzane.

6. Posiadacie Państwo prawo do: żądania od Administratora dostępu do danych osobowych, prawo do ich sprostowania, usunięcia lub ograniczenia przetwarzania, prawo do wniesienia sprzeciwu wobec przetwarzania, a także prawo do przenoszenia danych.
7. Macie Państwo prawo wniesienia skargi do UODO, gdy uzasadnione jest, że Pana/Pani dane osobowe przetwarzane są przez administratora niezgodnie z ogólnym rozporządzeniem o ochronie danych osobowych z dnia 27 kwietnia 2016r.
8. Kontakt z Inspektorem Ochrony Danych możliwy jest za pomocą poczty elektronicznej, adres:
   - Joanna Fikiel [tel: 18 414 00 17, e-mail: joanna@zmlesniak.pl]
   - zastępca IOD: Piotr Leśniak [tel: 604 113 952, e:mail: piotr@zmlesniak.pl]
   lub pisemnie na adres: Zakłady Mięsne Leśniak z siedzibą w Nowym Sączu, 33-300 Nowy Sącz, ul. Axentowicza 20A, dopisek: ochrona danych osobowych.

8.8 ZAŁĄCZNIK. WZÓR OBOWIĄZKU INFORMACYJNEGO W ZAKRESIE MONITORINGU WIDEO (CCTV)

Propozycja treści na tabliczki monitoringu:

Administratorem rejestrowanych danych jest Firma Zakłady Mięsne Leśniak z siedzibą w Nowym Sączu, 33-300 Nowy Sącz, ul. Axentowicza 20A.

Propozycja spełnienia obowiązku informacyjnego – monitoring wizyjny – tabliczka na ladę

Obiekt monitorowany wizyjnie

Szanowni Państwo,

Uprzejmie informujemy, że obiekty Zakładów Mięsnych Leśniak są monitorowane wizyjnie. Zbierane dane pozwalają na identyfikację osób, w związku z powyższym zgodnie z art. 13 ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. informujemy:

1. Administratorem danych osobowych jest Firma Zakłady Mięsne Leśniak z siedzibą w Nowym Sączu, 33-300 Nowy Sącz, ul. Axentowicza 20A, numer identyfikacji podatkowej NIP: 734-000-04-51.
2. Państwa dane osobowe przetwarzane będą w celu ochrony przed zagrożeniami zewnętrznymi oraz wewnętrznymi (zwiększenie bezpieczeństwa pracowników oraz bezpieczeństwa technologicznego) na podstawie art. 6 ust. 1 lit. f) ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r.,
3. Dane mogą być powierzane podmiotom serwisującym system monitoringu wizyjnego w celu naprawy i konserwacji urządzeń,
4. Dane mogą być udostępniane Organom ścigania w celu dochodzenia praw Administratora w przypadku popełnienia wykroczeń lub przestępstw na terenie monitorowanym,
5. Nagrania z monitoringu będą przechowywane przez okres do 21 dni,
6. Posiada Pani/Pan prawo do: żądania od administratora dostępu do danych osobowych, prawo do ich sprostowania, usunięcia lub ograniczenia przetwarzania, prawo do wniesienia sprzeciwu wobec przetwarzania, a także prawo do przenoszenia danych,
7. Ma Pan/Pani prawo wniesienia skargi do UODO, gdy uzasadnione jest, że Pana/Pani dane osobowe przetwarzane są przez administratora niezgodnie z ogólnym rozporządzeniem o ochronie danych osobowych z dnia 27 kwietnia 2016 r.

8.9 ZAŁĄCZNIK. WZÓR OBOWIĄZKU INFORMACYJNEGO DLA PRACOWNIKÓW W PRZYPADKU UŻYTKOWANIA SYSTEMU MONITORINGU CCTV

W związku z wejściem w życie z dniem 24 maja 2018 nowej Ustawy o Ochronie Danych Osobowych (Dz.U. 2018 poz. 1000) w Kodeksie Pracy wprowadzono nowe regulacje:

Art. 111. *W ustawie z dnia 26 czerwca 1974 r. – Kodeks pracy (Dz. U. z 2018 r. poz. 917) po art. 22^1 dodaje się art. 22^2 i art. 22^3 w brzmieniu:*
„Art. 22^2.
§ 1. Jeżeli jest to niezbędne do zapewnienia bezpieczeństwa pracowników lub ochrony mienia lub kontroli produkcji lub zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę, pracodawca może wprowadzić szczególny nadzór nad terenem zakładu pracy lub terenem wokół zakładu pracy w postaci środków technicznych umożliwiających rejestrację obrazu (monitoring).
§ 2. Monitoring nie obejmuje pomieszczeń sanitarnych, szatni, stołówek oraz palarni lub pomieszczeń udostępnianych zakładowej organizacji związkowej, chyba że stosowanie monitoringu w tych pomieszczeniach jest niezbędne do realizacji celu określonego w § 1 i nie naruszy to godności oraz innych dóbr osobistych pracownika, a także zasady wolności i niezależności związków zawodowych, w szczególności poprzez zastosowanie technik uniemożliwiających rozpoznanie przebywających w tych pomieszczeniach osób.
§ 3. Nagrania obrazu pracodawca przetwarza wyłącznie do celów, dla których zostały zebrane, i przechowuje przez okres nieprzekraczający 3 miesięcy od dnia nagrania.
§ 4. W przypadku, w którym nagrania obrazu stanowią dowód w postępowaniu prowadzonym na podstawie prawa lub pracodawca powziął wiadomość, iż mogą one stanowić dowód w postępowaniu, termin określony w § 3 ulega przedłużeniu do czasu prawomocnego zakończenia postępowania.
§ 5. Po upływie okresów, o których mowa w § 3 lub 4, uzyskane w wyniku monitoringu nagrania obrazu zawierające dane osobowe podlegają zniszczeniu, o ile przepisy odrębne nie stanowią inaczej.
§ 6. Cele, zakres oraz sposób zastosowania monitoringu ustala się w układzie zbiorowym pracy lub w regulaminie pracy albo w obwieszczeniu, jeżeli pracodawca nie jest objęty układem zbiorowym pracy lub nie jest obowiązany do ustalenia regulaminu pracy.
§ 7. Pracodawca informuje pracowników o wprowadzeniu monitoringu, w sposób przyjęty u danego pracodawcy, nie później niż 2 tygodnie przed jego uruchomieniem.
§ 8. Pracodawca przed dopuszczeniem pracownika do pracy przekazuje mu na piśmie informacje, o których mowa w § 6.
§ 9. W przypadku wprowadzenia monitoringu pracodawca oznacza pomieszczenia i teren monitorowany w sposób widoczny i czytelny, za pomocą odpowiednich znaków lub ogłoszeń dźwiękowych, nie później niż jeden dzień przed jego uruchomieniem.
§ 10. Przepis § 9 nie narusza przepisów art. 12 i art. 13 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) (Dz. Urz. UE L 119 z 04.05.2016, str. 1).
Art. 22^3.
§ 1. Jeżeli jest to niezbędne do zapewnienia organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy oraz właściwego użytkowania udostępnionych pracownikowi narzędzi pracy, pracodawca może wprowadzić kontrolę służbowej poczty elektronicznej pracownika (monitoring poczty elektronicznej).
§ 2. Monitoring poczty elektronicznej nie może naruszać tajemnicy korespondencji oraz innych dóbr osobistych pracownika.
§ 3. Przepisy art. 222 § 6–10 stosuje się odpowiednio.
§ 4. Przepisy § 1–3 stosuje się odpowiednio do innych form monitoringu niż określone w § 1, jeśli ich zastosowanie jest konieczne do realizacji celów określonych w § 1.”.

OBOWIĄZEK INFORMACYJNY DLA PRACOWNIKÓW
Obiekt monitorowany wizyjnie

Obiekty Zakładów Mięsnych są monitorowane wizyjnie. Zbierane dane pozwalają na identyfikację osób, w związku z powyższym zgodnie z art. 13 ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r oraz art. 22^2 Kodeksu pracy (Dz. U. z 2018 r. poz. 917). informuję:

Cel monitoringu:
Monitoring wizyjny służy do zapewnienia bezpieczeństwa pracowników oraz mienia firmy, zapewnienia kontroli produkcji, zapewnienia zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę.

Zakres monitorowanych obszarów:

Monitoring wizyjny obejmuje następujące pomieszczenia/lokalizacje:

a) obszar przed wejściem do zakładu i sklepu, obszar parkingu, warsztatu, rampa, przyjęcie półtusz,
b) obszar w obrębie recepcji, pomieszczenie działu fakturowania, kasa,
c) korytarze na wszystkich piętrach budynku,
d) hala ekspedycji, magazyn wyrobów, paczkarnia,
e) hale rozbiorowe i produkcyjne, wędzarnia, kotłownia, myjka pojemników.

Sposób monitorowania:
Monitorowanie odbywa się kamerami na zasadzie detekcji ruchu (obraz zostaje nagrany w momencie wykrycia ruchu). Kamery zostały umiejscowione w taki sposób, aby nie naruszać godności osób monitorowanych. Nagrania z monitoringu są przechowywane i odpowiednio zabezpieczone przez okres maksymalny do 21 dni, po czym są automatycznie usuwane. Dostęp do danych z monitoringu posiadają wyłącznie osoby upoważnione przez Administratora.

Dodatkowe Informacje
Administratorem Państwa danych osobowych jest Firma Zakłady Mięsne Wiesław Leśniak z siedzibą w Nowym Sączu, 33-300 Nowy Sącz, ul. Axentowicza 20A.
Dane z monitoringu mogą być powierzane podmiotom serwisującym system monitoringu wizyjnego w celu naprawy i konserwacji urządzeń.
Dane mogą być udostępniane Organom ścigania w celu dochodzenia praw Administratora w przypadku popełnienia wykroczeń lub przestępstw na terenie monitorowanym.
Posiada Pani/Pan prawo do: żądania od Administratora dostępu do danych osobowych, prawo do ich sprostowania, usunięcia lub ograniczenia przetwarzania, prawo do wniesienia sprzeciwu wobec przetwarzania, a także prawo do przenoszenia danych.
Ma Pan/Pani prawo wniesienia skargi do UODO, gdy uzasadnione jest, że Pana/Pani dane osobowe przetwarzane są przez administratora niezgodnie z ogólnym rozporządzeniem o ochronie danych osobowych z dnia 27 kwietnia 2016 r.

Oświadczam, że zostałem zapoznany z powyższą informacją

…… ……

Miejscowość i Data *Czytelny podpis pracownika*

8.10 ZAŁĄCZNIK. OGÓLNY OBOWIĄZEK INFORMACYJNY DLA PRACOWNIKÓW

OBOWIĄZEK INFORMACYJNY DLA PRACOWNIKÓW
Zasady przetwarzania danych osobowych – ogólnie

Ochrona danych osobowych – wypełnienie obowiązku informacyjnego

Administratorem moich danych osobowych jest Firma Zakłady Mięsne Leśniak z siedzibą w Nowym Sączu, 33-300 Nowy Sącz, ul. Axentowicza 20A.

W jakim celu Firma Zakłady Mięsne Leśniak przetwarza dane osobowe:
- w celu podjęcia działań przed zawarciem umowy oraz w celu zawarcia i realizacji umowy,
- w celach informacyjnych i marketingowych, wyłącznie na podstawie zgody zgodnie z treścią udzielonej zgody.
- w celu ochrony przed zagrożeniami zewnętrznymi oraz wewnętrznymi (zwiększenie bezpieczeństwa pracowników oraz bezpieczeństwa technologicznego)
- w celu zatrudniania pracowników i prowadzenia procesów rekrutacji

Jak długo przetwarzamy dane osobowe:
W zależności od celu przetwarzania dane osobowe będą przechowywane:
- przez okres trwania umowy oraz po zakończeniu jej trwania w celu wypełnienia obowiązku prawnego ciążącego na Administratorze,
- na czas zgodny z obowiązującymi przepisami prawa
- w przypadku prawnie usprawiedliwionych celów Administratora, w tym sprzedaży i marketingu bezpośredniego, do czasu cofnięcia przez osobę której dane dotyczą zgody.
- W przypadku monitoringi wideo (CCTV) przez okres do 21 dni.

Komu powierzamy i udostępniamy dane osobowe:
Pozyskanych danych osobowych nie udostępniamy i nie przekazujemy innym podmiotom. W szczególnych przypadkach (wykroczenia lub przestępstwa) dane mogą być udostępnione organom ścigania. Dane mogą być także udostępniane organom Państwa wyłącznie na podstawie przepisów prawa.
Dane osobowe możemy powierzyć do przetwarzania w naszym imieniu podmiotom realizującym dla nas usługi wspierające np. podwykonawstwo, hostowane strony internetowej, wysyłka newslettera, świadczenie usług księgowych, obsługa serwisowa naszych systemów informatycznych. W takim przypadku nadal jesteśmy Administratorem danych i odpowiadamy za przetwarzanie danych .

Prawa które przysługują osobie której dane przetwarzamy:
Osoba fizyczna ma prawo dostępu do treści swoich danych osobowych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przenoszenia danych, prawo do wniesienia sprzeciwu, prawo do cofnięcia zgody w dowolnym momencie.
Osoba fizyczna ma prawo wniesienia skargi do Urzędu Ochrony Danych Osobowych, gdy uzna, że przetwarzanie jej danych osobowych narusza przepisy rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 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) (Dz. Urz. UE L 119 z 4.05.2016).

Oświadczam, że zostałem zapoznany z powyższą informacją

…… ……
Miejscowość i Data *Czytelny podpis pracownika*

8.11 ZAŁĄCZNIK. WYTYCZNE DOTYCZĄCE ZATRUDNIANIA PRACOWNIKÓW

Propozycja zasad spełnienia obowiązku zgody i informacyjnego przy ogłoszeniach o pracę:

Ogłoszenie o pracy w gazecie/portalu lokalnym/itp:

Firma Zakłady Mięsne Leśniak z siedzibą w Nowym Sączu, 33-300 Nowy Sącz, ul. Axentowicza 20A,

poszukuje pracowników na stanowisko:

Np. Pracownik Biura Obsługi Klienta

Szczegółowe informacje oraz warunki aplikowania dostępne są w Sekretariacie firmy.

Dokumenty można składać:

1. Elektronicznie (skan) na adres e-mail: kadry@zmlesniak.pl

2. Osobiście w dziale kadrowym firmy

3. Pocztą tradycyjną na adres: ul. Axentowicza 20A, 33-300 Nowy Sącz

W dziale kadrowym dajemy do wypełnienia kwestionariusz ubiegającego się o zatrudnienia zawierający oświadczenie o zapoznaniu się z zasadami przetwarzania danych osobowych.

W przypadku gdy:

- **przyjdą dokumenty pocztą email bez oświadczenia**

możemy w drodze wyjątku w odpowiedzi wysłać maila z prośbą przysłanie oświadczenia w terminie 14 dni (druk dajemy w załączniku) z informacją, iż w przypadku braku skanu podpisanego oświadczenia, dokumenty aplikacyjne będą zniszczone.

- **przyjdą dokumenty pocztą tradycyjną bez oświadczenia**

możemy w drodze wyjątku skontaktować się z osobą np. telefonicznie i poinformować o konieczności uzupełnienia dokumentów o oświadczenie.

Klauzula zgody wraz z obowiązkiem informacyjnym

(do umieszczenia na stronie www jako plik: klauzula-oswiadczenie.pdf)

Zgoda na przetwarzanie danych osobowych

Poniższa zgoda na przetwarzanie Pani/Pana danych osobowych **jest niezbędna** abyśmy mogli rozpatrzyć Państwa kandydaturę:

Wyrażam zgodę na przetwarzanie moich danych osobowych, zawartych w dokumentach aplikacyjnych przez Zakłady Mięsne Leśniak w celu przeprowadzenia obecnego postępowania rekrutacyjnego.

……

Czytelny podpis kandydata do pracy

Poniższa zgoda na przetwarzanie Pani/Pana danych osobowych do przyszłych rekrutacji **nie jest wymagana**, jej wyrażenie pozwoli nam na wzięcie pod uwagę Państwa kandydatury w przyszłych rekrutacjach na podobne stanowiska pracy i przetwarzanie w tym celu Pani/Pana danych osobowych:

Wyrażam zgodę na przetwarzanie moich danych osobowych, zawartych w dokumentach aplikacyjnych przez Zakłady Mięsne Leśniak w kolejnych naborach kandydatów na pracowników Zakłady Mięsne Wiesław Leśniak.

……

Czytelny podpis kandydata do pracy

Prosimy o zapoznanie się z poniższymi zasadami przetwarzania danych osobowych i podpisanie oświadczenia.

Oświadczam, iż zostałem poinformowany o tym że:

Administratorem danych osobowych przetwarzanych w ramach procesów rekrutacji jest Firma Zakłady Mięsne Leśniak z siedzibą w Nowym Sączu, 33-300 Nowy Sącz, ul. Axentowicza 20A, numer identyfikacji podatkowej NIP: 734-000-04-51. Kontakt z Administratorem Danych jest możliwy pod adresem siedziby firmy oraz na adres email: biuro@zmlesniak.pl

Dane osobowe (oraz dane do kontaktu - o ile zostaną podane) będą przetwarzane w celu przeprowadzenia obecnego postępowania rekrutacyjnego, a w przypadku wyrażenia zgody, także w kolejnych naborach pracowników Zakładów Mięsnych Leśniak dna podstawie wyrażonej zgody (art. 6 ust. 1 lit. a RODO).

Osobie, której dane dotyczą przysługuje prawo do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem. W zakresie określonym prawem, dane mogą być przekazywane operatorom pocztowym, firmom kurierskim, podmiotom świadczącym na rzecz Zakładów Mięsnych Leśniak usługi doradcze, podmiotom zapewniającym obsługę informatyczną działalności Zakładów Mięsnych Leśniak oraz archiwom. Dane zgromadzone w procesach rekrutacyjnych będą przechowywane przez okres nie dłuższy niż 3 miesięcy.

Osobie, której dane dotyczą przysługuje prawo dostępu do swoich danych osobowych, żądania ich sprostowania lub usunięcia. Wniesienie żądania usunięcia danych jest równoznaczne z rezygnacją z udziału w procesie rekrutacji prowadzonym przez Zakłady Mięsne Leśniak. Ponadto przysługuje jej prawo do żądania ograniczenia przetwarzania w przypadkach określonych w art. 18 RODO.

Osobie, której dane dotyczą przysługuje prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych za niezgodne z prawem przetwarzanie jej danych osobowych. Podanie danych zawartych w dokumentach rekrutacyjnych nie jest obowiązkowe, jednak jest warunkiem umożliwiającym ubieganie się o przyjęcie kandydata do pracy w Zakładach Mięsnych Leśniak.

……
Czytelny podpis kandydata do pracy

Propozycja zasad procesu zatrudnienia pracownika i obsługi obecnych pracowników w związku z wymogami RODO:

Jakich dokumentów dotyczących RODO wymagamy przy zatrudnianiu pracowników:

Nowa Umowa o pracę / staż / praktyka:

a. Obowiązkowo wszyscy:
   - Podpisanie obowiązku informacyjnego ogólnego (wzór załącznik 8.10)
   - Podpisanie obowiązku informacyjnego o kamerach – gdy są stosowane (wzór załącznik 8.9)

b. Osoby zatrudniane na stanowiskach na których będą przetwarzać dane osobowe:
   - Odbycie szkolenia RODO
   - Podpisanie oświadczenia o poufności (wzór załącznik 8.3)
   - Wydanie upoważnienia do przetwarzania danych osobowych (wzór załącznik 8.2)

Umowa zlecenie:

a. Obowiązkowo wszyscy:
   - Podpisanie obowiązku informacyjnego ogólnego (wzór załącznik 8.10)
   - Podpisanie obowiązku informacyjnego o kamerach – gdy są stosowane (wzór załącznik 8.9)

b. Osoby zatrudniane na zleceniach na których będą przetwarzać dane osobowe:

   Jeżeli praca w siedzibie firmy:
   - Odbycie szkolenia RODO
   - Podpisanie oświadczenia o poufności (wzór załącznik 8.3)
   - Wydanie upoważnienia do przetwarzania danych osobowych (wzór załącznik 8.2)

   Jeżeli praca poza firmą (np. w domu):
   - Podpisanie umowy powierzenia danych do przetwarzania (wzór załącznik 8.4)

Umowy współpracy:

Umowy które wymagają przekazania/dostępu do danych osobowych:

- Podpisanie umowy powierzenia danych do przetwarzania (wzór załącznik 8.4)

Obecni pracownicy:

Należy wykonać kroki odpowiednio z punktu „**Nowa Umowa o pracę / staż / praktyka”** lub **„Umowa zlecenie”**

Propozycja nowego formularza dla kandydata do pracy:

Kwestionariusz osoby ubiegającej się o zatrudnienie (strona 1)

Część 1. Informacje podstawowe, podanie ich jest wymagane przez przepisy prawa

Imię (imiona) i nazwisko:	
Data urodzenia:	
Dane kontaktowe:	[Adres zamieszkania, numer telefonu]
Informacja o niepełnosprawności:	

Wykształcenie:	[Nazwa szkoły rok ukończenia, zawód specjalność, stopień naukowy, tytuł zawodowy]
Przebieg dotychczasowego zatrudnienia:	[okresy zatrudnienia u kolejnych pracodawców oraz zajmowane stanowiska]

Część 2. Informacje dodatkowe, podanie ich nie jest wymagane

Wykształcenie uzupełniające:	[kursy, studia podyplomowe, data ukończenia lub data rozpoczęcia jeżeli w trakcie]
Dodatkowe uprawnienia, umiejętności:	[wskazać jakie np. języki obce, prawo jazdy, itp.]

Część 3. Oświadczenia i zgody

Oświadczam, że dane wskazane przeze mnie w powyższym formularzu są zgodne z prawdą

……
Czytelny podpis kandydata do pracy

Wyrażam zgodę na przetwarzanie moich danych osobowych, zawartych w Części 2 formularza przez Zakłady Mięsne Wiesław Leśniak, w celu przeprowadzenia obecnego postępowania rekrutacyjnego.

……
Czytelny podpis kandydata do pracy

Prosimy o zapoznanie się z poniższymi zasadami przetwarzania danych osobowych i podpisanie oświadczenia

Oświadczam, iż zostałem poinformowany o tym że:
Administratorem danych osobowych przetwarzanych w ramach procesów rekrutacji jest Firma Zakłady Mięsne Leśniak z siedzibą w Nowym Sączu, 33-300 Nowy Sącz, ul. Axentowicza 20A. Kontakt z Administratorem Danych jest możliwy pod adresem siedziby firmy 33-300 Nowy Sącz, ul. Axentowicza 20A, email: biuro@zmlesniak.pl

Dane osobowe (oraz dane do kontaktu - o ile zostaną podane) będą przetwarzane w celu przeprowadzenia obecnego postępowania rekrutacyjnego na podstawie wymogów przepisu prawa oraz dobrowolnej zgody (art. 6 ust. 1 lit. a RODO).

Osobie, której dane dotyczą przysługuje prawo do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem. W zakresie określonym prawem, dane mogą być przekazywane operatorom pocztowym, firmom kurierskim, podmiotom świadczącym na rzecz Zakłady Mięsne Wiesław Leśniak usługi doradcze, podmiotom zapewniającym obsługę informatyczną działalności Zakłady Mięsne Wiesław Leśniak oraz archiwom. Dane zgromadzone w procesach rekrutacyjnych będą przechowywane przez okres nie dłuższy niż 3 miesięcy.

Osobie, której dane dotyczą przysługuje prawo dostępu do swoich danych osobowych, żądania ich sprostowania lub usunięcia. Wniesienie żądania usunięcia danych jest równoznaczne z rezygnacją z udziału w procesie rekrutacji prowadzonym przez Zakłady Mięsne Wiesław Leśniak. Ponadto przysługuje jej prawo do żądania ograniczenia przetwarzania w przypadkach określonych w art. 18 RODO.

Osobie, której dane dotyczą przysługuje prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych na niezgodne z prawem przetwarzanie jej danych osobowych. Podanie danych zawartych w dokumentach rekrutacyjnych nie jest obowiązkowe, jednak jest warunkiem umożliwiającym ubieganie się o przyjęcie kandydata do pracy w Zakłady Mięsne Wiesław Leśniak.

……
Czytelny podpis kandydata do pracy

Notatka służbowa (wypełnia pracownik kadr)

Data i godzina złożenia dokumentu:	
Sposób weryfikacji danych (z części 1 formularza):	Proszę opisać np. weryfikacja z dowodem osobistym, przegląd orzeczeń lekarskich
Podpis pracownika:	

8.12 ZAŁĄCZNIK. WZÓR ZGODY I OBOWIĄZKU INFORMACYJNEGO W PRYPADKU ZAPISU NA NEWSLETTER. – NIE DOTYCZY

Należy pozyskać 2 odrębne, dobrowolne zgody:

☐ Wyrażam zgodę na otrzymywanie drogą elektroniczną na wskazany przeze mnie adres e-mail informacji handlowej w rozumieniu art. 10 ust. 1 ustawy z dnia 18 lipca 2002 roku o świadczeniu usług drogą elektroniczną od Zakładów Mięsnych Leśniak z siedzibą w Nowym Sączu, 33-300 Nowy Sącz, ul. Axentowicza 20A.

☐ Wyrażam zgodę na przetwarzanie moich danych osobowych zgodnie z art. 13 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. oraz ustawy z dnia 16 lipca 2004 r. Prawo Telekomunikacyjne w celach marketingowych przez Zakłady Mięsne Leśniak z siedzibą w Nowym Sączu, 33-300 Nowy Sącz, ul. Axentowicza 20A i oświadczam, iż podanie przeze mnie danych osobowych jest dobrowolne oraz iż zostałem poinformowany o prawie żądania dostępu do moich danych osobowych, ich zmiany oraz usunięcia.

Nota informacyjna:

Zgodnie z art. 13 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016r. informuję, iż:

1) Administratorem danych osobowych jest firma Zakłady Mięsne Leśniak z siedzibą w Nowym Sączu, 33-300 Nowy Sącz, ul. Axentowicza 20A, numer identyfikacji podatkowej NIP: 734-000-04-51.
2) Pani/Pana dane osobowe przetwarzane będą w celu przesyłania informacji marketingowych, na podstawie art. 6 ust. 1 lit. a, Ogólnego Rozporządzenia o Ochronie Danych Osobowych z dnia 27 kwietnia 2016r.
3) Pani/Pana dane osobowe zostaną powierzone do przetwarzania firmie będącej naszym dostawcą usług związanych z obsługą wysyłki newslettera oraz hostowaniem systemu poczty e-mail wyłącznie w celu elektronicznego wprowadzenia i przechowywania do prowadzonego przez nas zbioru oraz wysyłki informacji.
4) Pani/Pana dane osobowe nie będą udostępniane innym podmiotom.
5) Pani/Pana dane osobowe przechowywane będą przez okres realizacji usług, do momentu wypisania się z newslettera.
6) Posiada Pani/Pan prawo do: żądania od Administratora dostępu do danych osobowych, prawo do ich sprostowania, usunięcia lub ograniczenia przetwarzania, prawo do wniesienia sprzeciwu wobec przetwarzania, a także prawo do przenoszenia danych.
7) Ma Pani/Pan prawo do wniesienia skargi do UODO. Gdy uzasadnione jest, że Pani/Pana dane osobowe przetwarzane są przez Administratora niezgodnie z Ogólnym Rozporządzeniem o Ochronie Danych Osobowych z dnia 27 kwietnia 2016r.
8) Podanie danych osobowych jest dobrowolne, jednakże niepodanie danych w zakresie wymaganym przez Administratora może skutkować brakiem możliwości wysyłki informacji.

03
REGULAMIN OCHRONY DANYCH OSOBOWYCH

Niniejszy regulamin stanowi wykaz podstawowych obowiązków z zakresu przestrzegania zasad ochrony danych osobowych zgodnie z przepisami RODO dla:

- Pracowników
- Współpracowników
- Pracowników podmiotów trzecich, posiadających dostęp do danych osobowych przetwarzanych przez Administratora
- Użytkowników systemów informatycznych z dostępem do danych osobowych przetwarzanych przez Administratora / Podmiot przetwarzający

Każda z w/w osób powinna zapoznać się z poniższym regulaminem oraz zobowiązać się do stosowania zasad w nim zawartych

1. ZASADY BEZPIECZNEGO UŻYTKOWANIA SPRZĘTU IT, DYSKÓW, PROGRAMÓW

1. W przypadku, gdy użytkownik przetwarzający dane osobowe korzysta ze sprzętu IT, zobowiązany jest do jego ochrony przed jakimkolwiek zniszczeniem lub uszkodzeniem. Za sprzęt IT rozumie się: komputery stacjonarne, monitory, drukarki, skanery, ksera, laptopy, służbowe tablety i smartfony
2. Użytkownik ma obowiązek natychmiast zgłosić zagubienie, utratę lub zniszczenie powierzonego mu Sprzętu IT
3. Samowolne otwieranie (demontaż) Sprzętu IT, instalowanie dodatkowych urządzeń (np. twardych dysków, pamięci) do lub podłączanie jakichkolwiek niezatwierdzonych urządzeń do systemu informatycznego jest zabronione
4. Użytkownik jest zobowiązany do uniemożliwienia osobom niepowołanym (np. klientom, pracownikom innych działów) wgląd do danych wyświetlanych na monitorach komputerowych – **tzw. Polityka czystego ekranu**
5. Przed czasowym opuszczeniem stanowiska pracy, użytkownik zobowiązany jest wywołać blokowany hasłem wygaszacz ekranu (WINDOS + L) lub wylogować się z systemu bądź z programu.
6. Po zakończeniu pracy, użytkownik zobowiązany jest:
    a. wylogować się z systemu informatycznego, a jeśli to wymagane - następnie wyłączyć sprzęt komputerowy
    b. zabezpieczyć stanowisko pracy, w szczególności wszelkie nośniki magnetyczne i optyczne na których znajdują się dane osobowe
7. Użytkownik jest zobowiązany do usuwania plików z nośników/dysków do których mają dostęp inni użytkownicy nieupoważnieni do dostępu do takich plików (np. podczas współużytkownania komputerów)
8. Osobą uprawnioną do niszczenia nośników jest ASI. ASI powinien TRWALE zniszczyć sam nośnik lub trwale usunąć z niego dane (np. zniszczenie płyt DVD w niszczarce, zniszczenie twardego dysku, pendrive młotkiem).
9. Użytkownicy komputerów przenośnych lub urządzeń mobilnych na których znajdują się dane osobowe lub z dostępem do danych osobowych przez Internet zobowiązani są do stosowania zasad bezpieczeństwa zawartych w Regulaminie korzystania z komputerów przenośnych oraz Regulaminie korzystania z urządzeń mobilnych

2. ZARZĄDZANIE UPRAWNIENIAMI

1. Każdy użytkownik z dostępem do danych osobowych (np. na swoim komputerze, na dysku sieciowym, w programie lub aplikacji, w poczcie elektronicznej) musi posiadać swój własny indywidualny identyfikator (login) do logowania się
2. Użytkownik otrzymuje dostęp i odpowiednie uprawnienia do zasobów i aplikacji na polecenie przełożonych i przy realizacji informatyków-administratorów
3. Użytkownicy nie mają prawa do samodzielnej zmiany uprawnień, np. przydzielenia sobie uprawnień administratora w Windows 7/10
4. Użytkowników obowiązuje zasada pracy na własnym koncie. Zabronione jest zatem umożliwianie innym osobom praca na koncie innego użytkownika

3. POLITYKA HASEŁ

1. Hasła powinny składać się z minimum 8 znaków
2. Hasła powinny zawierać duże litery + małe litery + cyfry (lub znaki specjalne)

3. Hasła nie mogą być łatwe do odgadnięcia. Nie powinny być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: dat, imion i nazwisk osób bliskich, imion zwierząt, popularnych dat, popularnych słów, typowych zestawów: 123456, qwerty
4. Hasła nie powinny być ujawnianie innym osobom. Nie należy zapisywać haseł na kartkach i w notesach, nie naklejać na monitorze komputera, nie trzymać pod klawiaturą lub w szufladzie
5. W przypadku ujawnienia hasła – należy natychmiast go zmienić
6. Hasła muszą być zmieniane co 6 miesięcy.
7. Jeżeli system nie wymusza zmiany haseł, użytkownik zobowiązany jest do samodzielnej zmiany hasła

4. ZABEZPIECZENIE DOKUMENTACJI PAPIEROWEJ Z DANYMI OSOBOWYMI

1. Upoważnieni pracownicy są zobowiązani do stosowania tzw. „**Polityki czystego biurka**”. Polega ona na zabezpieczaniu (zamykaniu) dokumentów np. w szafach, biurkach, pomieszczeniach przed kradzieżą lub wglądem osób nieupoważnionych po godzinach pracy lub podczas ich nieobecności w trakcie godzin pracy.
2. Upoważnieni pracownicy zobowiązani są do niszczenia dokumentów i wydruków w niszczarkach lub utylizacji ich w specjalnych bezpiecznych pojemnikach z przeznaczeniem do bezpiecznej utylizacji
3. Zabrania się pozostawiania dokumentów z danymi osobowymi poza zabezpieczonymi pomieszczeniami, np. w korytarzach, na kserokopiarkach, drukarkach, w pomieszczeniach konferencyjnych
4. Zabrania się wyrzucania niezniszczonych dokumentów na śmietnik lub porzucania ich na zewnątrz, np., na terenach publicznych miejskich lub w lesie.

5. ZASADY WYNOSZENIA NOŚNIKÓW Z DANYMI POZA FIRMĘ/ORGANIZACJĘ

1. Użytkownicy nie mogą wynosić na zewnątrz organizacji wymiennych elektronicznych nośników informacji z zapisanymi danymi osobowymi bez zgody Pracodawcy. Do takich nośników zalicza się: wymienne twarde dyski, pendrive, płyty CD, DVD, pamięci typu Flash a także dane przechowywane w tzw. chmurach (usługi typu Dropbox, OneDrive, Google Drive, itp.)
2. Dane osobowe wynoszone poza organizację muszą być zaszyfrowane (szyfrowane dyski, zahasłowane pliki)
3. Należy zapewnić bezpieczne przewożenie dokumentacji papierowej w plecakach, teczkach
4. Należy korzystać ze sprawdzonych firm kurierskich
5. W przypadku, gdy dokumenty przewozi pracownik, zobowiązany jest do zabezpieczenia przewożonych dokumentów przed zagubieniem i kradzieżą

6. ZASADY KORZYSTANIA Z INTERNETU

1. Użytkownik zobowiązany jest do korzystania z Internetu wyłącznie w celach służbowych
2. Zabrania się zgrywania na dysk twardy komputera oraz uruchamia jakichkolwiek programów nielegalnych oraz plików pobranych z niewiadomego źródła. Pliki takie powinny być ściągane tylko za każdorazową zgodą osoby upoważnionej do administrowania infrastrukturą IT (np. ASI) i tylko w uzasadnionych przypadkach
3. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie instalowane z Internetu
4. Zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hackerskim, pornograficznym, lub innym zakazanym przez prawo (na większości

stron tego typu jest zainstalowane szkodliwe oprogramowanie infekujące w sposób automatyczny system operacyjny komputera szkodliwym oprogramowaniem)
5. Nie należy w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł
6. W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy zwracać uwagę na pojawienie się odpowiedniej ikonki (kłódka) oraz adresu www rozpoczynającego się frazą ”https:”. Dla pewności należy „kliknąć” na ikonkę kłódki i sprawdzić, czy właścicielem certyfikatu jest wiarygodny właściciel
7. Należy zachować szczególną ostrożność w przypadku podejrzanego żądania lub prośby zalogowania się na stronę (np. na stronę banku, portalu społecznościowego, e-sklepu, poczty mailowej) lub podania naszych loginów i haseł, PIN-ów, numerów kart płatniczych przez Internet. Szczególnie tyczy się to żądania podania takich informacji przez rzekomy bank.

7. ZASADY KORZYSTANIA Z POCZTY ELEKTRONICZNEJ

1. Przesyłanie danych osobowych z użyciem maila poza organizację może odbywać się tylko przez osoby do tego upoważnione
2. W przypadku przesyłania danych osobowych poza organizację należy wykorzystywać mechanizmy kryptograficzne (hasłowanie wysyłanych dokumentów lub plików zzipowanych, podpis elektroniczny)
3. W przypadku zabezpieczenia plików hasłem, obowiązuje minimum 12 znaków: duże i małe litery i cyfry lub znaki specjalne a hasło należy przesłać inną metodą, np. telefonicznie lub SMS-em. Dopuszczone jest ustalenie jednego stałego hasła dla danego odbiorcy. Hasło takie powinno być zmieniane co 6 miesięcy. Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu
4. Zaleca się, aby użytkownik podczas przesyłania danych osobowych mailem zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata
5. **WAŻNE:** Nie należy otwierać załączników (plików) w mailach nawet od rzekomo znanych nam nadawców bez weryfikacji tegoż nadawcy. Tego typu maile większości przypadków zawierają załączniki ze szkodliwymi programami, które po „kliknięciu” infekują komputer użytkownika oraz często pozostałe komputery w sieci. W wyniku działania takiego szkodliwego oprogramowania może dojść do poważnych incydentów, łącznie z pełną utratą danych osobowych lub zaszyfrowanie ich przez kryptowirusy
6. **WAŻNE:** Bez weryfikacji wiarygodności nadawcy, nie należy „klikać” na hiperlinki w mailach, gdyż mogą to być hiperlinki do stron zainfekowanych lub niebezpiecznych. Użytkownik „klikając” na taki hiperlink bezwiednie infekuje swój komputer oraz często pozostałe komputery w sieci. W wyniku takiej infekcji może dojść do poważnych incydentów, łącznie z pełną utratą danych osobowych lub zaszyfrowanie m przez kryptowirusy
7. Należy zgłaszać informatykowi przypadki podejrzanych emaili
8. Użytkownicy nie powinni rozsyłać „niezawodowych” emaili w formie „łańcuszków szczęścia", np. Życzenia Świąteczne adresowane do 230 osób.
9. Podczas wysyłania maili do wielu adresatów jednocześnie, należy użyć metody „Ukryte do wiadomości – UDW”. Zabronione jest rozsyłanie korespondencji email z adresami w polu DW w następujących przypadkach: kiedy wysyłamy korespondencję poza organizację (do zewnętrznych odbiorców) oraz kiedy wysyłamy informację do osoby wewnątrz organizacji a zakres informacji wymaga poufności.
   W przypadku konieczności wysłania wiadomości do kilku odbiorców np. 3 wewnątrz firmy i 2 zewnętrznych adresy osób, które mają otrzymać kopię wiadomość należy umieścić w polu UDW (ang. BCC).
10. Użytkownicy nie powinni rozsyłać, maili zawierających załączniki o dużym rozmiarze
11. Użytkownicy powinni okresowo kasować niepotrzebne maile

12. Mail służbowy jest przeznaczony wyłącznie do wykonywania obowiązków służbowych
13. Zakazuje się wysyłania korespondencji służbowej na prywatne skrzynki pocztowe pracowników lub innych osób
14. Użytkownicy mają prawo korzystać z poczty mailowej dla celów prywatnych wyłącznie okazjonalnie i powinno być to ograniczone do niezbędnego minimum.
15. Korzystanie z maila dla celów prywatnych nie może wpływać na jakość i ilość świadczonej przez Użytkownika pracy oraz na prawidłowe i rzetelne wykonywanie przez niego obowiązków służbowych
16. Przy korzystaniu z maila, Użytkownicy mają obowiązek przestrzegać prawa własności przemysłowej i prawa autorskiego
17. Użytkownicy nie mają prawa korzystać z maila w celu rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec powszechnie obowiązujących zasad postępowania
18. Użytkownik bez zgody Administratora nie ma prawa wysyłać wiadomości zawierających dane osobowe dotyczące Administratora, jego pracowników, klientów, dostawców lub kontrahentów za pośrednictwem Internetu, w tym przy użyciu prywatnej elektronicznej skrzynki pocztowej

8. OCHRONA ANTYWIRUSOWA

1. Użytkownicy zobowiązani są do skanowania plików wprowadzanych z zewnętrznych nośników programem antywirusowym, jeśli system antywirusowy taką funkcje posiada
2. Zakazane jest wyłączanie systemu antywirusowego podczas pracy systemu informatycznego przetwarzającego dane osobowe
3. W przypadku stwierdzenia zainfekowania systemu lub pojawienia się komunikatów „np.; Twój system jest zainfekowany!, zainstaluj program antywirusowy", użytkownik obowiązany jest poinformować niezwłocznie o tym fakcie Informatyka lub osobę upoważnioną.

9. SKRÓCONA INSTRUKCJA POSTĘPOWANIA W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do powiadomienia Administratora w przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych
2. Do sytuacji wymagających powiadomienia, należą:
    a. niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów
    b. niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych
    c. nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka / ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek)
3. Do incydentów wymagających powiadomienia, należą:
    a. zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności)
    b. zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata / zagubienie danych)
    c. umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania)
4. Typowe przykłady incydentów wymagające reakcji:

a. ślady na drzwiach, oknach i szafach wskazują na próbę włamania
b. dokumentacja jest niszczona bez użycia niszczarki
c. fizyczna obecność w budynku lub pomieszczeniach osób zachowujących się podejrzanie
d. otwarte drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe
e. ustawienie monitorów pozwala na wgląd osób postronnych w dane osobowe
f. wynoszenie danych osobowych w wersji papierowej i elektronicznej na zewnątrz organizacji bez upoważnienia Administratora
g. udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej i ustnej
h. telefoniczne próby wyłudzenia danych osobowych
i. kradzież, zagubienie komputerów lub CD, twardych dysków, Pen-drive z danymi osobowymi
j. maile zachęcające do ujawnienia identyfikatora i/lub hasła,
k. pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów
l. hasła do systemów przyklejone są w pobliżu komputera

10. OBOWIĄZEK ZACHOWANIA POUFNOŚCI I OCHRONY DANYCH OSOBOWYCH

1. Każda z osób dopuszczona do przetwarzania danych osobowych jest zobowiązana do:
    a. przetwarzania danych osobowych wyłącznie w zakresie i celu przewidzianym w powierzonych przez Administratora zadaniach
    b. zachowania w tajemnicy danych osobowych do których mam lub będzie miał/a dostęp w związku z wykonywaniem zadań powierzonych przez Administratora
    c. niewykorzystywania danych osobowych w celach niezgodnych z zakresem i celem powierzonych zadań przez Administratora
    d. zachowania w tajemnicy sposobów zabezpieczenia danych osobowych
    e. ochrony danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją danych osobowych, nieuprawnionym ujawnieniem danych osobowych, nieuprawnionym dostępem do danych osobowych oraz przetwarzaniem
2. Jeśli jest to przewidziane, osoba dopuszczona do przetwarzania odbywa szkolenie z zasad ochrony danych osobowych
3. Osoby zapoznane z treścią niniejszego Regulaminu ODO lub przeszkolone zobowiązane są podpisać Oświadczenie o poufności
4. Zabrania się przekazywania bezpośrednio lub przez telefon danych osobowych osobom nieupoważnionym lub osobom których tożsamości nie można zweryfikować lub osobom podszywającym się pod kogoś innego
5. Zabrania się przekazywania lub ujawniania danych osobom lub instytucjom, które nie mogą wykazać się jasną podstawą prawną do dostępu do takich danych

11. POSTĘPOWANIE DYSCYPLINARNE

1. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych lub naruszenie zasad współpracy
2. Postępowanie sprzeczne z powyższymi zobowiązaniami, może też być uznane przez Administratora za naruszenie przepisów karnych zawartych w ogólnym Rozporządzeniu o ochronie danych UE z dnia 27 kwietnia 2016 r.

04
REGULAMIN KORZYSTANIA Z KOMPUTERÓW PRZENOŚNYCH

1. Każdy Użytkownik komputera przenośnego winien zapoznać się z Regulaminem użytkowania komputerów przenośnych oraz pisemnie zobowiązać się do jego przestrzegania.
2. W przypadku przechowywania na komputerze przenośnym danych osobowych lub stanowiących tajemnicę Pracodawcy, Użytkownik zobowiązany jest do ich przechowywania na dysku szyfrowanym, zabezpieczonym co najmniej 12 znakowym hasłem (duże, małe litery, znaki specjalne lub cyfry).
3. Na komputerach przenośnych przeznaczonych do zewnętrznych prezentacji multimedialnych nie powinny, o ile jest to możliwe, znajdować się dane osobowe lub stanowiące tajemnicę Pracodawcy.
4. W przypadku kradzieży lub zgubienia komputera przenośnego, Użytkownik powinien natychmiast powiadomić o tym Administratora zaznaczając jednocześnie, jakiego rodzaju dane były na tym urządzeniu przechowywane.
5. Użytkownik zobowiązany jest do zabezpieczenia komputera przenośnego w czasie transportu, a w szczególności:
a) zaleca się przenoszenie go w specjalnym futerale. *Dobrym sposobem na zmylenie potencjalnego złodzieja jest przenoszenie komputera przenośnego w zwykłej teczce-aktówce. Sugeruje to przenoszenie dokumentów a ukrywa fakt transportu komputera przenośnego.*
b) zabrania się pozostawiania komputera przenośnego w samochodzie podczas postoju w miejscu publicznym bez nadzoru. *W chwili obecnej złodzieje dysponują aparaturą umożliwiającą wykrywanie nawet ukrytych komputerów przenośnych.*
c) podczas jazdy samochodem zaleca się przechowywanie komputera przenośnego pod siedzeniem kierowcy lub pasażera. *Zabrania się przewożenia go np. na siedzeniach, co może skutkować kradzieżą na skrzyżowaniach, przejściach dla pieszych lub w korkach*.
6. W przypadku, gdy komputer przenośny pozostawiony jest w miejscu dostępnym dla osób nieupoważnionych, Użytkownik jest zobowiązany do stosowania linki zabezpieczającej. W szczególności dotyczy to zabezpieczenia komputera na stanowisku pracy, podczas konferencji, prezentacji, szkoleń, targów itp.
7. W przypadku pozostawiania komputerów przenośnych w biurze (np. w trakcie dłuższych przerw i po zakończeniu pracy), należy się wylogować i wyłączyć urządzenie.
8. Użytkownik komputera przenośnego jest zobowiązany do regularnego tworzenia kopii bezpieczeństwa danych na serwerze lub na określonych nośnikach (pendrive, CD, DVD). Nośniki z takimi kopiami powinny być przechowywane w bezpiecznym miejscu, z uwzględnieniem ochrony przed dostępem osób niepowołanych.
9. Pracując na komputerze przenośnym w miejscach publicznych i środkach transportu, Użytkownik zobowiązany jest chronić wyświetlane na monitorze informacje przed wglądem osób nieupoważnionych.

Oświadczenie pracownika:

Zapoznałem się z treścią Regulaminu użytkowania komputerów przenośnych i zobowiązuję się do przestrzegania zasad w nim zawartych

Czytelny podpis Użytkownika

05
REGULAMIN KORZYSTANIA Z URZĄDZEŃ MOBILNYCH

1. Każdy Użytkownik urządzenia mobilnego (smartfon, tablet, smartwatch, terminal, itp.) winien zapoznać się z Regulaminem użytkowania urządzeń mobilnych oraz pisemnie zobowiązać się do jego przestrzegania.

2. W przypadku przechowywania na urządzeniu mobilnym danych osobowych lub stanowiących tajemnicę Pracodawcy, Użytkownik zobowiązany jest do ich przechowywania na dysku szyfrowanym, zabezpieczonym hasłem (duże, małe litery, znaki specjalne lub cyfry) lub inna adekwatną metodą (odcisk palca, rozpoznawanie twarzy, złożony symbol graficzny.

3. Na urządzeniach mobilnych przeznaczonych do zewnętrznych prezentacji multimedialnych nie powinny, o ile jest to możliwe, znajdować się dane osobowe lub stanowiące tajemnicę Pracodawcy.

4. W przypadku kradzieży lub zgubienia urządzenia mobilnego, Użytkownik powinien natychmiast powiadomić o tym Administratora zaznaczając jednocześnie, jakiego rodzaju dane były na tym urządzeniu przechowywane.

5. Użytkownik zobowiązany jest do zabezpieczenia urządzenia mobilnego w czasie transportu, a w szczególności:
a) zaleca się przenoszenie go w specjalnym futerale.
b) zabrania się pozostawiania urządzenia przenośnego w samochodzie podczas postoju w miejscu publicznym bez nadzoru. *W chwili obecnej złodzieje dysponują aparaturą umożliwiającą wykrywanie nawet ukrytych urządzeń.*
c) podczas jazdy samochodem zaleca się przechowywanie urządzenia mobilnego w sposób ograniczający możliwość kradzieży podczas postoju. *Zabrania się przewożenia go np. na siedzeniach, co może skutkować kradzieżą na skrzyżowaniach, przejściach dla pieszych lub w korkach*.

6. Zabrania się pozostawiać urządzenia mobilnego bez nadzoru jest w miejscu dostępnym dla osób nieupoważnionych. W szczególności dotyczy to konferencji, prezentacji, szkoleń, targów itp.

7. Użytkownik urządzenia mobilnego jest zobowiązany do regularnego tworzenia kopii bezpieczeństwa danych na serwerze lub na określonych nośnikach (pendrive, CD, DVD). Nośniki z takimi kopiami powinny być przechowywane w bezpiecznym miejscu, z uwzględnieniem ochrony przed dostępem osób niepowołanych.

9. Pracując na urządzeniu mobilnym w miejscach publicznych i środkach transportu, Użytkownik zobowiązany jest chronić wyświetlane na nim informacje przed wglądem osób nieupoważnionych.

Oświadczenie pracownika:

Zapoznałem się z treścią Regulaminu użytkowania urządzeń mobilnych i zobowiązuję się do przestrzegania zasad w nim zawartych

Czytelny podpis Użytkownika