Rejestr czynności przetwarzania – Monitoring

I Administrator

1. Administratorem danych jest FIT FOOD GROUP S.A. z siedzibą w Kędzierzynie-Koźlu przy Al. Jana Pawła II 58 lok.A/VII, NIP: 749 202 20 79, wpisana do Krajowego Rejestru Sądowego pod numerem: 0000286132, przez Sąd Rejonowy w Opolu (zwana dalej: „Firmą).

II Cele przetwarzania danych

1. Zapewnienie bezpieczeństwa osób przebywających na terenie placówki (prewencja),
2. Ochrona mienia klientów placówki,
3. Jako materiał dowodowy dla organów ścigania, w przypadku złamania lub naruszenia prawa przez dowolną osobę przebywającą na terenie placówki

III Kategoria osób, których dane są przetwarzane

Firma przetwarza dane wszystkich osób znajdujących się na terenie i w przestrzeni wokół budynku będącej w zasięgu kamer.

IV Kategorie podmiotów, które posiadają dostęp do danych

Do danych osobowych dostęp posiada wyłącznie administrator. Członkowie zespołu Firmy mają ograniczony dostęp do poszczególnych kategorii danych poprzez ograniczenie uprawnień technicznych. Zewnętrznie do danych osobowych dostęp mają następujące podmioty:

Firma serwisująca kamery: https://lightsystem.pl/

Polityka prywatności każdego z tych podmiotów mieści się na ich stronach podanych powyżej.

Powyższe podmioty jako znajdujące się w obszarze EOG lub na liście Privacy Shield przestrzegają przepisów z zakresu danych osobowych analogicznych do Rozporządzenia tzw. RODO. Z podmiotami zawarte zostały umowy powierzenia, przeważnie w formie aktualizacji ich regulaminów.

V Kategorie danych

1. Administrator przetwarza następujące dane Klienta:
   a. czas pobytu na terenie placówki (godzina, dzień, rok),
   b. wizerunek osób przebywających na terenie placówki (w tym możliwość zarejestrowania cech charakterystycznych tj. tatuaż, ubiór fryzura, sposób poruszania się),
   c. zachowania osób zarejestrowane w trakcie pobytu w placówce,

   marka, model i numer rejestracyjny pojazdu znajdującego się w polu widzenia kamery.

Administrator zastrzega, że powyżej wymienione dane są zbierane mimowolnie poprzez znajdujący się na terenie monitoring. Celem monitoringu jest przede wszystkim zapewnienie bezpieczeństwa osobą znajdującym się na terenie placówki. Dla pracowników zespół przetwarzanych danych wynika z przepisów kadrowych. Dane z monitoringu nie będą w żadnym razie profilowane i powiązywane z danymi klientów w których posiadaniu jest administrator. Dostęp do danych mogą otrzymać organy ścigania wyłącznie na wniosek wynikający z przepisów prawa.

2. Dla pracowników zespół przetwarzanych danych wynika z przepisów kadrowych.

VI Przechowywanie danych

1. Okres przechowywania danych, nie będzie dłuższy niż 30 dni lub
2. Dane osób przebywających na terenie placówki przechowywane będą do wniosku o ich usunięcie,
3. W sytuacjach spornych lub zagrażających bezpieczeństwu administrator zastrzega sobie prawo przetrzymywania materiałów na czas niezbędny do rozstrzygnięcia sporu po wcześniejszej modyfikacji treści tak, by usunąć z niej wszelkie cechy danych osobowych. Administrator zobowiązuje się do niezwłoczne go usunięcia materiałów po zakończenia sporu lub po usunięciu ewentualnego zagrożenia.

Firma zobowiązuje się do niszczenia powstałych tymczasowo materiałów zawierających dane osobowe oraz dbałości o obieg danych i ich minimalizację zgodnie z poniższymi procedurami.

VII Techniczne i organizacyjne środki bezpieczeństwa

1. Przez bezpieczeństwo informacji rozumie się zapewnienie:
   a. uniemożliwienia dostępu do danych osobom trzecim;
   b. uniknięcia nieautoryzowanych zmian w danych;

c. zapewnienia dostępu do danych, w każdym momencie żądanym przez użytkownika

2. Jako dane podlegające szczególnej ochronie (informacje poufne) rozumie się:
   a. informacje o realizowanych kontraktach (zarówno planowane, bieżące jak i historyczne),
   b. informacje finansowe Firmy,
   c. dane osobowe.

VIII Zasada minimalnych uprawnień

1. W ramach nadawania uprawnień przetwarzanych danych należy stosować zasadę „minimalnych uprawnień", to znaczy przydzielać minimalne uprawnienia, które są konieczne do wykonywania pracy na danym stanowisku.

   Przykładowo:
   pracując na komputerze PC każdy pracownik powinien posiadać tylko takie uprawnienia jakie są wymagane do realizacji swoich obowiązków (a nie na przykład uprawnienia administracyjne).

IX Zasada zabezpieczeń

System IT Firmy powinien być chroniony celem uzyskania skutecznej ochrony danych.

Przykładowo:
w celu ochrony przed wirusami stosuje się równolegle wiele technik: oprogramowanie antywirusowe, systemy typu firewall, odpowiednią konfigurację systemu aktualizacji Windows.

X Dostęp do danych poufnych na stacjach PC

Dostęp do danych poufnych w LAN realizowany jest na przeznaczonych do tego serwerach.

XI Publiczne udostępnianie infrastruktury IT

Infrastruktura udostępniona publicznie musi być szczególnie zabezpieczona.
Przykładowe środki bezpieczeństwa:

a. separacja od sieci LAN
b. wykonanie hardeningu systemu (zwiększenia bezpieczeństwa oferowanego domyślne przez system)

XII Kopie zapasowe

1. Każde istotne dane (w tym dane poufne) powinny być archiwizowane na wypadek awarii w firmowej infrastrukturze IT.
2. Nośniki z kopiami zapasowymi powinny być przechowywane w miejscu uniemożliwiającym dostęp osobom nieupoważnionym.
3. Okresowo kopie zapasowe muszą być testowane pod względem rzeczywistej możliwości odtworzenia danych.

XIII Dostęp do systemów IT po zakończeniu współpracy

W przypadku rozwiązania współpracy pracownika z Firmą niezwłocznie dezaktywowane są wszelakie jego dostępy w systemach IT oraz w terminie 1 roku od dnia rozwiązania współpracy dezaktywowane są indywidualnie przyporządkowane do pracownika adresy e-mail.

XIV Zabezpieczenie stacji roboczych

1. Stacje robocze powinny być zabezpieczone przed nieautoryzowanych dostępem osób trzecich. Minimalne środki ochrony to:
   a. zainstalowane na stacjach systemy typu: firewall oraz antywirus,
   b. wdrożony system aktualizacji systemu operacyjnego oraz jego składników,
   c. wymaganie podania hasła przed uzyskaniem dostępu do stacji,
   d. bieżąca praca z wykorzystaniem konta nieposiadającego uprawnień administracyjnych.

XV Wykorzystanie haseł

1. Hasła powinny być okresowo zmieniane.
2. Hasła nie mogą być przechowywane w formie otwartej (nie zaszyfrowanej).
3. Nie wolno przekazywać hasła osobom trzecim.
4. Hasła nie powinny być łatwe do odgadnięcia, to znaczy:
   a. powinny składać się z minimum 8 znaków, w tym jeden znak specjalny, cyfra i wielka litera,
   b. nie może być słowem żadnego języka.

XVI Odpowiedzialność pracowników za dane poufne

Pracownicy zobowiązani są do strzeżenie danych poufnych, w tym osobowych.

XVII Odpowiedzialność pracowników za dane dostępowe do systemów

1. Każdy pracownik zobowiązany jest do ochrony swoich danych dostępowych do systemów informatycznych. Dane dostępowe obejmują między innymi takie elementy jak:
    a. hasła dostępowe,
    b. klucze softwareowe (pliki umożliwiające dostęp - np. *certyfikaty do VPN*) oraz sprzętowe,
    c. inne mechanizmy umożliwiające dostęp do systemów IT.

XVIII Przykłady ochrony danych dostępowych

nieprzekazywanie dostępów do systemów IT innym osobom (np. przekazywanie swojego hasła dostępowego osobom trzecim),
nieprzechowywanie danych w miejscach publicznych (np. zapisywanie haseł dostępowych w łatwo dostępnych miejscach),
ochrona danych dostępowych przed kradzieżą przez osoby trzecie.

XIX Systemy IT/serwery

Systemy IT przechowujące dane poufne (np. dane osobowe) muszą być odpowiednio zabezpieczone. W szczególności należy dbać o poufność, integralność i rozliczalność danych przetwarzanych w systemach.

XX Ograniczony dostęp do biura

Dostęp do budynku Firmy jest ograniczony poprzez drzwi wejściowe, recepcję i system monitoringu.

XXI Naruszenie danych osobowych

Pracownik zobowiązany jest do poinformowania o naruszeniu w ciągu 24 godzin. O ile wystąpi taka konieczność zgłoszenie naruszenia danych osobowych następuje w ciągu 48 godzin od daty powzięcia informacji o powyżej wymienionym zdarzeniu, zgodnie z poniżej przedstawionym schematem.

XXII Formularze

Raport z naruszenia ochrony danych osobowych w Firmie powinien zawierać następujące informacje:

1. data, godzina
2. dane osoby powiadamiającej o zaistniałym zdarzeniu (imię, nazwisko, stanowisko służbowe, nazwa użytkownika (jeżeli występuje)
3. lokalizacja zdarzenia: (np. numer pokoju, nazwa pomieszczenia, nazwa bazy danych)
4. rodzaj naruszenia bezpieczeństwa
5. podjęte działania
6. przyczyny wystąpienia zdarzenia
7. postępowanie wyjaśniające
8. podjęte środki techniczne, organizacyjne i dyscyplinarne w celu zapobiegania w przyszłości podobnych naruszeń ochrony danych osobowych.

XXIII Prawo do usunięcia/zmiany danych

Jeśli klient chce usunąć swoje dane przetwarzane przez Firmę powinien stawić się w siedzibie firmy osobiście w celu weryfikacji danych – niemożliwa jest weryfikacja np. poprzez PESEL, ponieważ Firma go nie pobiera.

Firma usuwa dane z **systemów IT** *usuwamy wszystkie nagrania, które zawierają wizerunek klienta.*

XXIV Wgląd do danych osobistych

Jeśli jakikolwiek podmiot, którego dane są przetwarzane przez Firmę chce otrzymać wgląd do swoich danych i je poprawić/zaktualizować, powinien stawić się w siedzibie firmy osobiście w celu weryfikacji danych – niemożliwa jest weryfikacja np. poprzez PESEL, ponieważ Firma go nie pobiera. Następnie po jego weryfikacji, dane klienta zostaną niezwłocznie zmienione/podane.

XXV Procedura przeniesienia danych klienta

W sytuacji gdy klient zgłosi się z prośbą o przeniesienie jego danych do innej firmy, z którą aktualnie nawiązał współpracę, musi się on zgłosić się osobiście z podaniem adresu e-mail na który mają te dane zostać przez Firmę wysłane, a następnie po jego weryfikacji, dane klienta zostaną niezwłocznie zmienione/podane.

Wdrożono:……..
(podpis osoby wdrażającej)