

Załącznik nr 4 do zapytania ofertowego nr 1/2026**POLITYKA OCHRONY DANYCH OSOBOWYCH****GASTRONOM P.H. Paweł Hurkała**

Dokument wewnętrzny

opracowany z uwzględnieniem projektu cyfryzacji i wdrożenia ERP

Nazwa dokumentu	Polityka ochrony danych osobowych
Administrator danych	GASTRONOM P.H. Paweł Hurkała
Siedziba	ul. Goleniowska 63b, 70-847 Szczecin
Zakres	obszar kadrowy, handlowy, produkcyjny, logistyczny, monitoring, systemy IT i postępowania ofertowe
Powiązanie z projektem	Wdrożenie systemów cyfrowych dla standaryzacji produkcji i poprawy jakości dań gotowych
Środowisko IT	serwer lokalny / infrastruktura on- premises



1. Cel i charakter dokumentu

Niniejsza Polityka określa zasady organizacyjne, techniczne i prawne dotyczące przetwarzania danych osobowych w przedsiębiorstwie GASTRONOM P.H. Paweł Hurkała. Dokument ma charakter wdrożeniowy i dowodowy: porządkuje sposób postępowania z danymi osobowymi, wskazuje role i odpowiedzialności, opisuje podstawowe środki bezpieczeństwa oraz stanowi podstawę wykazania zgodności przetwarzania danych z RODO.

Polityka została opracowana z uwzględnieniem faktycznego modelu działalności przedsiębiorstwa oraz dokumentacji projektu dotyczącego wdrożenia systemów cyfrowych, w szczególności planowanego wdrożenia systemu ERP, rejestracji danych produkcyjnych i magazynowych w czasie rzeczywistym, monitoringu, lokalnej infrastruktury serwerowej oraz współpracy z podmiotami zewnętrznymi.

2. Podstawy prawne

- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. (RODO).
- Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych.
- Kodeks pracy, w szczególności przepisy dotyczące monitoringu wizyjnego pracowników.
- Przepisy szczególne z zakresu prawa pracy, ubezpieczeń społecznych, rachunkowości, podatków oraz archiwizacji dokumentacji.

3. Zakres stosowania

Polityka ma zastosowanie do wszystkich procesów, w których przedsiębiorstwo przetwarza dane osobowe, niezależnie od formy ich utrwalenia, miejsca przetwarzania oraz nośnika. Dotyczy ona w szczególności:

- dokumentacji papierowej, korespondencji i formularzy;
- systemów informatycznych, w tym systemu ERP, programów kadrowo-płacowych, systemów księgowych, poczty elektronicznej, plików roboczych oraz rejestrów pomocniczych;
- przetwarzania danych pracowników, zleceniobiorców, pracowników agencji pracy, kontrahentów, przedstawicieli kontrahentów, klientów, przewoźników, oferentów i innych osób kontaktowych;
- monitoringu wizyjnego na terenie zakładu oraz terenu wokół zakładu, jeżeli pozostaje on w zasięgu kamer;
- współpracy z podmiotami przetwarzającymi dane w imieniu Administratora.



4. Definicje

Pojęcie	Znaczenie
Administrator	GASTRONOM P.H. Paweł Hurkała z siedzibą w Szczecinie przy ul. Goleniowskiej 63b.
RODO	rozporządzenie UE 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych.
Dane osobowe	wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.
Przetwarzanie	każda operacja wykonywana na danych, w tym zbieranie, utrwalanie, organizowanie, przechowywanie, modyfikowanie, przeglądanie, udostępnianie, usuwanie lub niszczenie.
Podmiot przetwarzający	podmiot zewnętrzny przetwarzający dane w imieniu Administratora na podstawie umowy powierzenia.
Naruszenie ochrony danych	naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub dostępu do danych.

5. Administrator danych i role w organizacji

- Administratorem danych osobowych jest GASTRONOM P.H. Paweł Hurkała, ul. Goleniowska 63b, 70-847 Szczecin, e-mail: biuro@daniagastronom.pl.
- Na dzień przyjęcia niniejszej Polityki Administrator nie wyznaczył Inspektora Ochrony Danych. Ocena obowiązku wyznaczenia IOD podlega okresowej weryfikacji, w szczególności w przypadku zmiany skali, rodzaju lub ryzyka przetwarzania.
- Za organizację zgodności z RODO odpowiada Administrator lub osoby przez niego wyznaczone, odpowiednio do zakresu obowiązków.
- Osoby mające dostęp do danych osobowych przetwarzają je wyłącznie na podstawie upoważnienia, polecenia Administratora albo w zakresie wynikającym z ich roli służbowej i obowiązków ustawowych.



6. Kategorie osób, danych i procesów przetwarzania

W przedsiębiorstwie przetwarzane są dane osobowe w następujących głównych obszarach:

Obszar	Kategorie osób	Zakres danych
Kadry i płace	pracownicy zatrudnieni na podstawie umów o pracę (ok. 20 osób), kandydaci do pracy, osoby uprawnione do świadczeń, dane członków rodzin, jeżeli wynikają z obowiązków pracodawcy.	dane identyfikacyjne, kontaktowe, kadrowe, płacowe, ewidencja czasu pracy, badania i szkolenia wymagane przepisami.
Umowy cywilnoprawne	zleceniobiorcy (ok. 60 osób) oraz osoby współpracujące na podstawie innych umów cywilnoprawnych.	dane identyfikacyjne, kontaktowe, rozliczeniowe, podatkowe, ubezpieczeniowe.
Personel agencyjny	osoby kierowane do pracy przez agencje pracy tymczasowej (ok. 30 osób równolegle, zależnie od okresu).	dane niezbędne do organizacji pracy, identyfikacji, bezpieczeństwa, ewidencji wejść, wykonywania zadań i współpracy z agencją.
Kontrahenci i osoby kontaktowe	dostawcy, odbiorcy, przewoźnicy, przedstawiciele handlowi, osoby składające zamówienia i reklamacje.	dane identyfikacyjne i służbowe, dane kontaktowe, dane związane z realizacją umów i historią współpracy.
Postępowania ofertowe i projektowe	oferenci, wykonawcy, osoby reprezentujące podmioty biorące udział w postępowaniach związanych z projektem i bieżącą działalnością.	dane identyfikacyjne, kontaktowe, dane zawarte w ofertach, pełnomocnictwach, oświadczeniach i korespondencji.
Systemy produkcyjne i magazynowe	użytkownicy systemu ERP, operatorzy terminali, pracownicy magazynu, produkcji i administracji.	identyfikatory użytkowników, logi, dane operacyjne przypisane do użytkownika, informacje o partiach, zleceniach i operacjach.
Monitoring wizyjny	pracownicy, goście, dostawcy, odbiorcy, kierowcy, osoby wchodzące na teren zakładu lub	wizerunek, data i godzina zdarzenia, ewentualnie numery rejestracyjne





Fundusze Europejskie
dla Pomorza Zachodniego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Pomorze
Zachodnie

	pozostające w zasięgu kamer.	pojazdów, jeśli mieszczą się w kadrze.
--	------------------------------	--

7. Cele i podstawy prawne przetwarzania

Przetwarzanie danych osobowych odbywa się wyłącznie w zakresie niezbędnym do realizacji określonych celów. Główne cele i podstawy prawne przedstawia poniższa tabela:

Cel przetwarzania	Podstawa prawna
Zawarcie i wykonywanie umów handlowych oraz zamówień	art. 6 ust. 1 lit. b RODO
Realizacja obowiązków pracodawcy oraz obowiązków podatkowych, ubezpieczeniowych, rachunkowych i archiwizacyjnych	art. 6 ust. 1 lit. c RODO
Organizacja pracy, bezpieczeństwo, ochrona mienia, dochodzenie roszczeń i obrona przed roszczeniami, prowadzenie monitoringu, bezpieczeństwo systemów i sieci	art. 6 ust. 1 lit. f RODO
Prowadzenie postępowań ofertowych i dokumentowanie ich przebiegu	art. 6 ust. 1 lit. c lub f RODO - zależnie od trybu i celu postępowania
W sytuacjach szczególnych, gdy jest to wymagane	art. 6 ust. 1 lit. a RODO - zgoda, przy czym zgoda nie jest domyślną podstawą w relacjach pracowniczych i kontraktowych

8. Zasady przetwarzania danych

- legalności, rzetelności i przejrzystości - dane są przetwarzane na podstawie właściwej podstawy prawnej i przy zapewnieniu osobom wymaganych informacji;
- ograniczenia celu - dane są zbierane dla wyraźnych, prawnie uzasadnionych celów i nie są dalej przetwarzane w sposób niezgodny z tymi celami;
- minimalizacji danych - zakres danych jest adekwatny, stosowny i ograniczony do tego, co niezbędne;
- prawidłowości - Administrator podejmuje działania zapewniające aktualność i poprawność danych;
- ograniczenia przechowywania - dane są przechowywane nie dłużej niż jest to niezbędne;
- integralności i poufności - dane są odpowiednio zabezpieczone przed utratą, ujawnieniem lub nieuprawnionym dostępem;

- rozliczalności - Administrator musi być w stanie wykazać przestrzeganie zasad RODO.

9. Środowisko przetwarzania danych i architektura IT

Przetwarzanie danych w przedsiębiorstwie odbywa się zarówno w formie papierowej, jak i elektronicznej. W związku z realizowanym projektem cyfryzacji środowisko elektroniczne ma charakter kluczowy i obejmuje system ERP wdrażany do obsługi produkcji, magazynu, logistyki, sprzedaży, księgowości oraz analiz biznesowych.

- system ERP i powiązane moduły funkcjonujące na lokalnej infrastrukturze serwerowej (on-premises), z możliwością współpracy z terminalami, wagami, czytnikami kodów i urządzeniami mobilnymi;
- stacje robocze użytkowników objęte centralnym zarządzaniem aktualizacjami, polityką hasel i ochroną antywirusową;
- sieć przewodowa oraz przemysłowe Wi-Fi wspierające rejestrację danych na hali produkcyjnej i w magazynie;
- kopie zapasowe realizowane według przyjętych zasad bezpieczeństwa, z okresową weryfikacją możliwości odtworzenia danych;
- role i uprawnienia przypisane do użytkowników w zależności od działu i zakresu obowiązków.

Administrator dąży do zapewnienia zgodności rozwiązań IT z zasadą privacy by design i privacy by default, tj. uwzględniania ochrony danych już na etapie projektowania i konfiguracji procesów, ról, formularzy, raportów i integracji.

10. Upoważnienia, dostęp i środki bezpieczeństwa

1. Dostęp do danych osobowych mają wyłącznie osoby, którym jest on potrzebny do wykonywania obowiązków służbowych lub ustawowych.
2. Administrator stosuje zasadę najmniejszych uprawnień - użytkownik otrzymuje wyłącznie taki zakres dostępu, jaki jest niezbędny do jego pracy.
3. Dostęp do systemów informatycznych odbywa się przy użyciu indywidualnych identyfikatorów i hasel. Zabrania się współdzielenia kont użytkowników, chyba że wynika to z uzasadnionych ograniczeń technicznych i zostało formalnie zatwierdzone.
4. Upoważnienia są nadawane, zmieniane i odbierane w sposób kontrolowany, zwłaszcza przy zmianie stanowiska, zakończeniu współpracy lub stwierdzeniu incydentu bezpieczeństwa.
5. W przedsiębiorstwie stosuje się odpowiednie środki organizacyjne i techniczne, adekwatne do ryzyka, w tym w szczególności:
 - kontrolę dostępu do pomieszczeń, serwera, dokumentacji papierowej i stanowisk pracy;
 - zabezpieczenie pomieszczeń i urządzeń przed dostępem osób nieupoważnionych;



- aktualizacje systemów i oprogramowania, ochronę antywirusową, zabezpieczenia sieciowe oraz kopie zapasowe;
- podział uprawnień zgodnie z rolami oraz rejestrowanie wybranych operacji użytkowników;
- okresowe przeglądy przyjętych środków bezpieczeństwa oraz reakcję na wykryte podatności lub incydenty.

6. Dokumentacja papierowa zawierająca dane osobowe jest przechowywana w sposób ograniczający dostęp osób nieuprawnionych, w szczególności w zamkniętych pomieszczeniach, szafach lub strefach administracyjnych.

11. Podmioty przetwarzające i udostępnianie danych

1. Administrator może korzystać z usług podmiotów zewnętrznych wspierających działalność, jeżeli jest to uzasadnione biznesowo lub technicznie.

2. Jeżeli podmiot zewnętrzny przetwarza dane osobowe w imieniu Administratora, współpraca wymaga zawarcia umowy powierzenia przetwarzania danych albo innego udokumentowanego instrumentu spełniającego wymagania RODO.

3. Przed powierzeniem danych Administrator ocenia, czy dany podmiot daje wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych.


4. Dane mogą być przekazywane w szczególności:

- biurowi rachunkowemu i doradcom, w zakresie niezbędnym do realizacji obowiązków księgowych, kadrowych, prawnych i podatkowych;
- dostawcom systemów informatycznych, wsparcia serwisowego, utrzymania infrastruktury oraz wdrożenia ERP;
- agencjom pracy i kontrahentom - w zakresie niezbędnym do organizacji pracy, współpracy handlowej lub logistycznej;
- organom publicznym, sądom, urządowi i innym podmiotom uprawnionym na podstawie przepisów prawa.

5. Co do zasady Administrator nie zakłada przekazywania danych do państw trzecich lub organizacji międzynarodowych. Jeżeli dojdzie do takiego przekazania, nastąpi ono wyłącznie na podstawie odpowiedniego mechanizmu przewidzianego w RODO i z zachowaniem obowiązków informacyjnych.

12. Monitoring wizyjny

1. Na terenie zakładu stosowany jest monitoring wizyjny w celu zapewnienia bezpieczeństwa osób, ochrony mienia, kontroli dostępu do stref istotnych dla działalności oraz w razie potrzeby ustalenia przebiegu zdarzeń.



2. Monitoring nie może naruszać godności ani innych dóbr osobistych pracowników i innych osób znajdujących się w zasięgu kamer. Nie służy on stałej, nadmiernej kontroli jakości wykonywania pracy.

3. Wdrożenie monitoringu oraz jego zasady są komunikowane osobom objętym monitoringiem zgodnie z przepisami prawa pracy i zasadami przejrzystości. Teren monitorowany powinien być oznaczony w sposób widoczny i czytelny.

4. Nagrania przechowywane są przez okres nie dłuższy niż 3 miesiące, chyba że stanowią dowód w postępowaniu lub Administrator powziął wiadomość, że mogą stanowić dowód - wtedy okres przechowywania ulega przedłużeniu do czasu prawomocnego zakończenia postępowania.

5. Dostęp do nagrań mają wyłącznie osoby upoważnione. Udostępnienie nagrań następuje tylko wtedy, gdy istnieje odpowiednia podstawa prawna albo prawnie uzasadniony cel ich wykorzystania.

13. Okresy przechowywania danych

Dane osobowe są przechowywane przez okres wynikający z celu przetwarzania, przepisów prawa oraz uzasadnionej potrzeby zabezpieczenia interesów Administratora. Orientacyjne okresy przedstawia tabela:

Kategoria	Okres / zasada retencji
Dokumentacja pracownicza	zgodnie z przepisami prawa pracy i przepisami szczególnymi dotyczącymi dokumentacji pracowniczej
Dokumentacja księgowa i podatkowa	przez okres wymagany przepisami podatkowymi, rachunkowymi i archiwizacyjnymi
Dane kontrahentów i osób kontaktowych	przez czas trwania współpracy, a następnie do upływu terminów przedawnienia roszczeń oraz obowiązków dowodowych
Dokumenty ofertowe i projektowe	przez okres niezbędny do przeprowadzenia postępowania, realizacji umowy, kontroli projektu oraz wymaganych okresów archiwizacji
Nagrania z monitoringu	co do zasady do 3 miesięcy, z wyjątkiem sytuacji związanych z postępowaniami
Logi systemowe i konta użytkowników	przez okres uzasadniony bezpieczeństwem systemów, zasadami audytu oraz polityką retencji obowiązującą w danym systemie

19.11

14. Prawa osób, których dane dotyczą

Osobie, której dane dotyczą, przysługują - w zakresie przewidzianym przepisami - następujące prawa:

- prawo dostępu do danych i uzyskania ich kopii;
- prawo sprostowania danych nieprawidłowych lub uzupełnienia danych niekompletnych;
- prawo żądania usunięcia danych, jeżeli zachodzą przesłanki z RODO;
- prawo ograniczenia przetwarzania;
- prawo wniesienia sprzeciwu wobec przetwarzania opartego na prawnie uzasadnionym interesie;
- prawo przenoszenia danych, jeżeli przetwarzanie odbywa się na podstawie zgody lub umowy w sposób zautomatyzowany;
- prawo cofnięcia zgody - gdy przetwarzanie opiera się na zgodzie;
- prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.

Wnioski związane z realizacją praw należy kierować do Administratora na adres wskazany w niniejszej Polityce. Każdy wniosek podlega rejestracji, analizie i obsłudze w terminach wynikających z RODO.

15. Naruszenia ochrony danych i incydenty bezpieczeństwa

1. Każda osoba mająca dostęp do danych osobowych ma obowiązek niezwłocznie zgłosić Administratorowi lub osobie wyznaczonej wszelkie zdarzenia mogące skutkować naruszeniem ochrony danych.
2. Zgłoszeniu podlega w szczególności utrata nośnika, nieuprawniony dostęp, ujawnienie danych, błędna wysyłka dokumentów lub wiadomości, zainfekowanie urządzenia, uszkodzenie systemu, podejrzenie wycieku albo brak dostępności danych.
3. Po zgłoszeniu incydentu Administrator dokonuje analizy okoliczności, oceny ryzyka naruszenia praw lub wolności osób fizycznych, wdraża działania korygujące oraz dokumentuje przebieg sprawy.
4. Jeżeli naruszenie podlega zgłoszeniu organowi nadzorczemu lub osobom, których dane dotyczą, Administrator działa zgodnie z terminami i przesłankami określonymi w RODO.



16. Zasady ochrony danych przy wdrażaniu i zmianie systemów

1. Każda istotna zmiana procesu, systemu, integracji lub sposobu gromadzenia danych - w szczególności w projekcie cyfryzacji, wdrożeniu ERP, integracji z wagami, terminalami i urządzeniami mobilnymi - wymaga uwzględnienia ochrony danych już na etapie planowania.
2. Przed uruchomieniem nowego rozwiązania należy co najmniej:
 - określić cel i zakres przetwarzania;
 - zweryfikować podstawy prawne oraz minimalny zakres danych potrzebnych do osiągnięcia celu;
 - ustalić role i zakresy uprawnień użytkowników;
 - ocenić, czy nie zachodzi potrzeba zawarcia umów powierzenia lub aktualizacji istniejących umów;
 - ustalić zasady retencji, logowania operacji i kopii zapasowych;
 - zweryfikować, czy charakter przetwarzania wymaga przeprowadzenia oceny skutków dla ochrony danych.
3. Administrator dokumentuje działania dotyczące zgodności projektowanych rozwiązań z RODO, tak aby możliwe było wykazanie rozliczalności w razie audytu, kontroli lub sporu.

17. Szkolenia, poufność i przeglądy

1. Osoby dopuszczone do przetwarzania danych powinny zostać zapoznane z niniejszą Polityką, zasadami poufności oraz podstawowymi regułami bezpieczeństwa informacji.
2. W miarę potrzeb Administrator organizuje szkolenia lub instruktaż dotyczący ochrony danych, w szczególności dla osób korzystających z systemów ERP, systemów magazynowych, kadrowych oraz monitoringu.
3. Polityka i środki bezpieczeństwa podlegają okresowemu przeglądowi, zwłaszcza po zmianach organizacyjnych, wdrożeniu nowych narzędzi, incydencie bezpieczeństwa albo zmianie przepisów.

18. Postanowienia końcowe

1. Niniejsza Polityka wchodzi w życie z dniem jej zatwierdzenia przez Administratora.
2. Dokument ma zastosowanie we wszystkich jednostkach organizacyjnych przedsiębiorstwa oraz wobec wszystkich osób przetwarzających dane na polecenie Administratora.
3. Naruszenie zasad określonych w niniejszej Polityce może skutkować odpowiedzialnością porządkową, kontraktową albo inną przewidzianą przepisami prawa.





Fundusze Europejskie
dla Pomorza Zachodniego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Pomorze
Zachodnie

Data przyjęcia dokumentu	v. 22.04.2026
Podpis Administratora / osoby upoważnionej	v. Piotr Hunka
Podpis Wykonawcy/Dostawcy

ZAŁĄCZNIK NR 1

Informacja o zasadach przetwarzania danych osobowych dla oferentów, wykonawców, dostawców i osób reprezentujących te podmioty

1. Administratorem danych osobowych jest GASTRONOM P.H. Paweł Hurkała, ul. Goleniowska 63b, 70-847 Szczecin, e-mail: biuro@daniagastronom.pl.
2. Administrator nie wyznaczył Inspektora Ochrony Danych. W sprawach dotyczących przetwarzania danych można kontaktować się na wskazany adres e-mail.
3. Dane osobowe są przetwarzane w celu:
 - a. przeprowadzenia postępowania ofertowego lub zakupowego;
 - b. oceny ofert, prowadzenia korespondencji, wyjaśnień oraz dokumentowania przebiegu postępowania;
 - c. zawarcia i wykonania umowy;
 - d. wypełnienia obowiązków prawnych związanych z rachunkowością, podatkami, archiwizacją i kontrolą projektu;
 - e. ustalenia, dochodzenia lub obrony roszczeń.
4. Podstawą prawną przetwarzania jest art. 6 ust. 1 lit. b, c oraz f RODO, odpowiednio do etapu i celu współpracy.
5. Prawnie uzasadnionym interesem Administratora jest w szczególności zapewnienie prawidłowego przebiegu postępowania, kontakt z oferentami i wykonawcami, zabezpieczenie interesów majątkowych oraz wykazanie prawidłowości wydatkowania środków i realizacji projektu.
6. Odbiorcami danych mogą być podmioty świadczące usługi księgowe, prawne, IT, doradcze, instytucje finansujące projekt, organy kontrolne i inne podmioty uprawnione na podstawie przepisów prawa.
7. Dane nie są co do zasady przekazywane poza Europejski Obszar Gospodarczy. Jeżeli doszłoby do takiego przekazania, nastąpi ono wyłącznie na podstawie odpowiednich zabezpieczeń przewidzianych prawem.
8. Dane będą przechowywane przez okres niezbędny do przeprowadzenia postępowania, zawarcia i realizacji umowy, rozliczenia projektu, a następnie przez okres wymagany przepisami prawa i zasadami archiwizacji dokumentacji projektowej oraz dokumentacji księgowej.
9. Osobie, której dane dotyczą, przysługuje prawo dostępu do danych, sprostowania, ograniczenia przetwarzania, wniesienia sprzeciwu - w przypadkach przewidzianych prawem - oraz prawo wniesienia skargi do Prezesa UODO.
10. Podanie danych osobowych jest warunkiem niezbędnym do udziału w postępowaniu ofertowym lub realizacji współpracy w zakresie, w jakim dane te są wymagane przepisami, warunkami postępowania albo są niezbędne do zawarcia i wykonania umowy. Niepodanie danych może skutkować brakiem możliwości udziału w postępowaniu lub zawarcia umowy.
11. Dane nie są wykorzystywane do zautomatyzowanego podejmowania decyzji, w tym profilowania.

Podpis Administratora / osoby upoważnionej	✓ 22.04.2026 Paweł Hurkała
Podpis Wykonawcy/Dostawcy



Fundusze Europejskie
dla Pomorza Zachodniego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Pomorze
Zachodnie

ZAŁĄCZNIK NR 2

Skrócona informacja o monitoringu wizyjnym

1. Administratorem danych osobowych przetwarzanych w ramach monitoringu wizyjnego jest GASTRONOM P.H. Paweł Hurkata, ul. Goleniowska 63b, 70-847 Szczecin, e-mail: biuro@daniagastronom.pl.
2. Monitoring stosowany jest w celu zapewnienia bezpieczeństwa osób, ochrony mienia, kontroli dostępu do terenu zakładu oraz ustalenia przebiegu zdarzeń.
3. Zakres danych obejmuje wizerunek osób oraz inne informacje zarejestrowane przez kamery, w tym datę i godzinę zdarzenia; w razie objęcia kadrem pojazdu - również numer rejestracyjny.
4. Podstawą prawną przetwarzania jest art. 6 ust. 1 lit. f RODO oraz odpowiednie przepisy Kodeksu pracy, jeżeli monitoring obejmuje teren zakładu pracy.
5. Nagrania przechowuje się co do zasady przez okres nie dłuższy niż 3 miesiące, chyba że stanowią dowód w postępowaniu lub Administrator powziął wiadomość, że mogą taki dowód stanowić.
6. Osobie, której dane dotyczą, przysługuje prawo dostępu do danych, ograniczenia przetwarzania oraz wniesienia skargi do Prezesa UODO - w granicach przewidzianych przepisami.

Podpis Administratora / osoby upoważnionej	22.04.2016 Paweł Hurkata
Podpis Wykonawcy/Dostawcy