POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

Sprawdził:		**Data:**	
Zatwierdził:		**Data:**	
Obowiązuje od:			
Wymagania prawne:	„RODO", zwane także „GDPR" lub „Ogólnym Rozporządzeniem o Ochronie Danych", to Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych.		

SPIS TREŚCI:

1. Wykaz podstawowych skrótów

Skrót	Opis
RODO	Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. o Ochronie Danych
u.o.d.o.	Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2016 r. poz. 922)
UODO	Urząd Ochrony Danych Osobowych
ADO	Administrator Danych Osobowych
IOD	Inspektor Ochrony Danych
ASI	Administrator Systemów Informatycznych
SI	System Informatyczny
SZBDO	System Zarządzania Bezpieczeństwem Danych Osobowych
PBDO	Polityka Bezpieczeństwa Danych Osobowych
IZSI	Instrukcja Zarządzania Systemami Informatycznymi

2. Wykaz podstawowych definicji

Ilekroć w niniejszej Polityce Bezpieczeństwa mowa o:

1. **Administratorze Danych Osobowych** – rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę, decydujące o celach i środkach przetwarzania danych osobowych;
2. **Inspektor Ochrony Danych** – rozumie się przez to osobę wyznaczoną przez Administratora Danych Osobowych, nadzorującą przestrzeganie zasad;
3. **Administratorze Systemów Informatycznych** – rozumie się przez to wyznaczoną przez Administratora Danych Osobowych osobę lub podmiot zewnętrzny, odpowiedzialny za funkcjonowanie systemów i sieci teleinformatycznych oraz za przestrzeganie zasad i wymogów bezpieczeństwa systemów i sieci teleinformatycznych;
4. **Osobie upoważnionej** – rozumie się przez to osobę upoważnioną przez Administratora Danych Osobowych do przetwarzania danych osobowych. Użytkownikiem może być pracownik firmy, osoba wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilno-prawnej, a także osoba odbywająca wolontariat, praktykę lub staż.
5. **Danych osobowych** – rozumie się przez to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osoba możliwa do zidentyfikowania to osoba, której tożsamość można ustalić bezpośrednio lub pośrednio, szczególnie przez powołanie się na numer identyfikacyjny lub jeden bądź kilka szczególnych czynników określających jej fizyczną, umysłową, ekonomiczną, kulturową lub społeczną tożsamość;
6. **Zbiorze danych osobowych** – rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępny według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;
7. **Przetwarzaniu danych osobowych** – rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych;

8. **Systemie informatycznym** – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
9. **Zabezpieczeniu danych w systemie informatycznym** – rozumie się przez to wdrożenie i eksploatację stosowanych środków technicznych i organizacyjnych zapewniających ochronę danych osobowych przed ich nieuprawnionym przetwarzaniem;
10. **Bezpieczeństwie informacji** – rozumie się przez to zespół zasad, jakimi należy się kierować projektując oraz wykorzystując systemy i aplikacje służące do przetwarzania informacji by w każdych okolicznościach dostęp do nich był zgodny z założeniami;
11. **Usuwaniu danych** – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;
12. **Zgodzie osoby, której dane dotyczą** – rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie. Zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści. Zgoda może być odwołana w każdym czasie;
13. **Odbiorcy danych** – rozumie się przez to każdego, komu udostępnia się dane osobowe za wyjątkiem:
    - osoby, której dane dotyczą,
    - osoby upoważnionej do przetwarzania danych osobowych,
    - przedstawiciela, o którym mowa w art. 31a u.o.d.o.,
    - podmiotu, o którym mowa w art. 31 u.o.d.o.,
    - organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem;
14. **Państwie trzecim** – rozumie się przez to państwo należące do Europejskiego Obszaru Gospodarczego;
15. **Haśle** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie użytkownikowi uprawnionemu do pracy w systemie informatycznym;
16. **Identyfikatorze użytkownika** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych w wyznaczonych obszarach systemu informatycznego firmy;
17. **Poufności danych** – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom lub podmiotom;
18. **Integralności danych** – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
19. **Rozliczalności danych** – rozumie się przez to właściwość zapewniającą, że działania osoby lub podmiotu mogą być przypisane w sposób jednoznaczny tylko tej osobie lub podmiotowi;
20. **Użytkowniku systemu informatycznego** – rozumie się przez to osobę upoważnioną do przetwarzania danych osobowych w systemach informatycznych, której nadano unikalny identyfikator i hasło**;**
21. **Uwierzytelnieniu** – rozumie się przez to proces poprawnej identyfikacji użytkownika systemu informatycznego w stopniu umożliwiającym przyznanie odpowiednich uprawnień lub przywilejów w systemie informatycznym firmy;
22. **Incydencie** – rozumie się przez to naruszenie bezpieczeństwa danych osobowych ze względu na

poufność, dostępność i integralność;

23. **Zagrożeniu** - rozumie się przez to potencjalną możliwość wystąpienia incydentu;
24. **Działaniu korygującym** – rozumie się przez to działanie przeprowadzone w celu wyeliminowania przyczyny incydentu lub innej niepożądanej sytuacji;
25. **Działaniu zapobiegawczym** – rozumie się przez to działanie, które należy przedsięwziąć, aby wyeliminować przyczyny zagrożenia lub innej potencjalnej sytuacji niepożądanej.

3. Wprowadzenie

Polityka Bezpieczeństwa Danych Osobowych określa reguły przetwarzania danych osobowych oraz sposobów ich zabezpieczenia, jako zestaw praw, zasad i zaleceń regulujących sposób ich zarządzania, ochrony i dystrybucji w firmie Centrum Dystrybucji Mięsa i Wędlin P.H.U. SzynkoVit Dorota Polak-Wysocka.

Polityka zawiera informacje dotyczące rozpoznawania procesów przetwarzania danych osobowych oraz wprowadzonych zabezpieczeń techniczno-organizacyjnych, zapewniających ochronę przetwarzanych danych osobowych.

Niniejszy dokument jest zgodny z obowiązującymi przepisami prawa, a w szczególności z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. o Ochronie Danych.

4. Cele Polityki Bezpieczeństwa Danych Osobowych

Celem Polityki Bezpieczeństwa Danych Osobowych jest określenie oraz wdrożenie zasad bezpieczeństwa i ochrony danych osobowych przetwarzanych w firmie Centrum Dystrybucji Mięsa i Wędlin P.H.U. SzynkoVit Dorota Polak-Wysocka., a w szczególności:

1) przetwarzanie danych osobowych, których przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
2) nieprzetwarzanie szczególnych kategorii danych (wyznanie, orientacja seksualna, poglądy polityczne, pochodzenie, religia)
3) zapewnienie spełnienia wymagań prawnych;
4) zapewnienie poufności, integralności oraz rozliczalności danych osobowych przetwarzanych w firmie;
5) podnoszenie świadomości osób przetwarzających dane osobowe;
6) zaangażowanie osób przetwarzających dane osobowe firmy w ich ochronę.

5. Inspektor Ochrony Danych (IOD)

1) Administrator Danych Osobowych **nie powołuje** Inspektora Ochrony Danych (IOD). Firma Centrum

Dystrybucji Mięsa i Wędlin P.H.U. SzynkoVit Dorota Polak-Wysocka. nie przetwarza danych na dużą skalę, nie jest bankiem i nie prowadzi działalności ubezpieczeniowej oraz nie prowadzi usług medycznych. W związku z powyższym firma Centrum Dystrybucji Mięsa i Wędlin P.H.U. SzynkoVit Dorota Polak-Wysocka **nie powołuje** Inspektora Ochrony Danych (IOD)

6. Ogólna ocena ryzyka

1) Kontekst dla oceny ryzyka,
firma Centrum Dystrybucji Mięsa i Wędlin P.H.U. SzynkoVit Dorota Polak-Wysocka. nie przetwarza danych wrażliwych jak: dane o stanie zdrowia, informacje o adopcji, orientacji seksualnej, religii. Przetwarzanie danych wrażliwych wymaga spełnienia określonych warunków i ryzyko naruszenia praw jednostki w przypadku, gdy dane te wyciekną, jest znacznie większe, niż w przypadku przetwarzania przez firmę Centrum Dystrybucji Mięsa i Wędlin P.H.U. SzynkoVit Dorota Polak-Wysocka zwykłych danych (jak imię i nazwisko).

2) Opis i identyfikacja wymagań prawnych i techniczno-organizacyjnych,
Firma Centrum Dystrybucji Mięsa i Wędlin P.H.U. SzynkoVit Dorota Polak-Wysocka przetwarza dane w formie papierowej oraz na komputerach. Dane są przetwarzane zgodnie z prawem, w tym z adekwatnością celu i proporcjonalnością. Firma nie zbiera danych, których nie potrzebuje. Firma Centrum Dystrybucji Mięsa i Wędlin P.H.U. SzynkoVit Dorota Polak-Wysocka posiada własną infrastrukturę IT.

3) Szacowanie i ocena ryzyka;
Prawdopodobieństwo wystąpienia zdarzenia naruszającego prawa osób, których dane są przetwarzane jest: **bardzo niskie.**

4) Postępowanie z ryzykiem
Poprzez szkolenia pracowników upoważnionych do przetwarzania danych osobowych firma firma zmniejsza poziomu ryzyka

7. Analiza oceny skutków dla ochrony danych osobowych

1) W firmie Centrum Dystrybucji Mięsa i Wędlin P.H.U. SzynkoVit Dorota Polak-Wysocka przetwarzanie danych osobowych **nie powoduje** wysokiego ryzyka naruszenia praw lub wolności osób fizycznych (DPIA, od Data Protection Impact Assessment)

8. Osoby upoważnione do przetwarzania danych osobowych

1) Do obowiązków osób upoważnionych do przetwarzania danych osobowych należy:
   - zapoznanie się z przepisami prawa w zakresie ochrony danych osobowych oraz postanowieniami Polityki Bezpieczeństwa Danych Osobowych i Instrukcji Zarządzania Systemami Informatycznymi;
   - stosowanie się do zaleceń Administrator Danych Osobowych;
   - przetwarzania danych osobowych wyłącznie w zakresie ustalonym indywidualnie przez

Administratora Danych Osobowych i tylko w celu wykonywania nałożonych obowiązków służbowych;

- niezwłoczne informowanie Administrator Danych Osobowych o wszelkich nieprawidłowościach dotyczących bezpieczeństwa danych osobowych przetwarzanych w firmie;
- ochronę danych osobowych oraz środków wykorzystywanych do przetwarzania danych osobowych przed nieuprawnionym dostępem, ujawnieniem, modyfikacją, zniszczeniem lub zniekształceniem;
- korzystanie z systemów informatycznych firmy w sposób zgodny ze wskazówkami zawartymi w instrukcjach obsługi urządzeń wchodzących w skład systemów informatycznych;
- bezterminowe zachowanie w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia;
- zachowanie szczególnej staranności w trakcie wykonywania operacji przetwarzania danych osobowych w celu ochrony interesów osób, których dane dotyczą.

9. Podstawowe zasady ochrony danych osobowych

1) Wszystkie dane osobowe w firmie należy przetwarzać zgodnie z obowiązującymi przepisami prawa.
2) W stosunku do osób, których dane osobowe wrażliwe są przetwarzane należy spełnić obowiązek informacyjny wynikający z przepisów art 13 RODO.
3) Zebrane dane osobowe należy przetwarzać dla oznaczonych i zgodnych z prawem celów i nie poddawać dalszemu przetwarzaniu niezgodnemu z tymi celami.
4) Należy zadbać, aby przetwarzanie danych osobowych odbywało się zgodnie z zasadami dotyczącej merytorycznej poprawności oraz adekwatnie do celów w jakich zostały zebrane.
5) Dane osobowe w firmie można przetwarzać nie dłużej niż jest to niezbędne do osiągnięcia celu ich przetwarzania.
6) Należy zapewnić poufność, integralność oraz rozliczalność danych osobowych przetwarzanych w firmie.
7) Przetwarzane dane osobowe nie mogą być udostępniane bez zgody osób, których dane dotyczą, chyba że udostępnia się te dane osobom, których dane dotyczą, osobom upoważnionym do przetwarzania danych osobowych, podmiotom którym przekazano dane na podstawie umowy powierzenia oraz organom państwowym lub organom samorządu terytorialnego w związku z prowadzonym postępowaniem.
8) Przetwarzanie danych osobowych w firmie może odbywać się zarówno w systemach informatycznych, jak i w formie tradycyjnej: kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych.
9) W zakresie danych osobowych przetwarzanych w innych systemach niż informatyczne, obowiązują nadal dotychczasowe przepisy o tajemnicy służbowej, obiegu i zabezpieczaniu dokumentów służbowych.
10) Wszystkim osobom, których dane są przetwarzane przysługuje prawo do ochrony danych ich dotyczących, do kontroli przetwarzania tych danych oraz do ich uaktualniania, usunięcia jak również do uzyskiwania wszystkich informacji o przysługujących im prawach.
11) Należy zapewnić odpowiedni stopień bezpieczeństwa odpowiadający ustalonemu ryzyku. Firma stosuje rozwiązania o charakterze fizycznym poprzez przechowywanie dokumentacji w zamykanych

szafkach na klucz, oraz zamykanych pomieszczeniach na klucz. Archiwum jest zamykane i zabezpieczone kluczem elektronicznym. Środki organizacyjne jakie firma stosuje to polityka czystego biurka oraz obowiązek zmiany haseł dostępu.

10. Upoważnienie do przetwarzania danych osobowych

1) Do przetwarzania danych osobowych i obsługi zbiorów informatycznych zawierających te dane mogą być dopuszczone wyłącznie osoby posiadające upoważnienie do przetwarzania danych osobowych wydane przez Administratora Danych Osobowych.
2) Administrator Danych Osobowych prowadzi ewidencje osób upoważnionych do przetwarzania danych osobowych.

11. Powierzenie przetwarzania danych osobowych

1) Administrator Danych Osobowych może zlecić innemu podmiotowi przetwarzanie danych osobowych w celu realizacji określonego zadania.
2) W sytuacji powierzenia przetwarzania danych osobowych podmiotowi zewnętrznemu, w umowie powierzenia przetwarzania danych osobowych określa się przede wszystkim cel i zakres przetwarzania danych osobowych.

12. Udostępnianie danych osobowych

1) Administrator Bezpieczeństwa Informacji prowadzi ewidencję udostępniania danych osobowych instytucjom i osobom spoza firmy

13. Przekazywanie danych osobowych poza Polskę

Administrator Danych Osobowych może przekazywać dane osobowe do państw Europejskiego Obszaru Gospodarczego tylko wtedy, gdy na przekazanie danych osobowych wyrazi zgodę UODO.

14. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe

Administrator Danych Osobowych odpowiedzialny jest za prowadzenie i przechowywanie dokumentacji zawierającej wykaz budynków, pomieszczeń lub części pomieszczeń tworzący obszar, w którym przetwarzane są dane osobowe zarówno w formie papierowej jak i elektronicznej.

15. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych

Administrator Danych Osobowych odpowiedzialny jest za prowadzenie i przechowywanie dokumentacji zawierającej wykaz wszystkich zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych.

16. Opis struktury zbiorów danych osobowych

Administrator Danych Osobowych odpowiedzialny jest za prowadzenie i przechowywanie dokumentacji zawierającej opis struktury zbiorów danych osobowych przetwarzanych w firmie.

17. Opis sposobu przepływu danych pomiędzy poszczególnymi systemami

Administrator Danych Osobowych odpowiedzialny jest za prowadzenie i przechowywanie dokumentacji zawierającej opis sposobu przepływu danych pomiędzy poszczególnymi systemami.

18. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

Administrator Bezpieczeństwa Informacji odpowiedzialny jest za prowadzenie i przechowywanie dokumentacji zawierającej określone środki techniczne i organizacyjne niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

19. Anonimizacja danych

Zgodnie z art. 17 RODO, **każda osoba fizyczna może żądać „bycia zapomnianym”**
Osoba, której dane dotyczą, ma prawo żądać od administratora niezwłocznego usunięcia dotyczących jej danych osobowych, a administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe

20. Informacja o zasadach przetwarzania danych osobowych

Firma Centrum Dystrybucji Mięsa i Wędlin P.H.U. SzynkoVit Dorota Polak-Wysocka zatrudnia poniżej 250 osób co zwalnia firmę z obowiązku informowania swoich klientów, kto jest administratorem danych, w jakim celu są one zbierane oraz przez jaki czas będą przechowywane (Art 13 RODO).

21. Postanowienia końcowe

W sprawach nieuregulowanych w niniejszej Polityce Bezpieczeństwa Danych Osobowych mają zastosowanie przepisy Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. o Ochronie Danych