

POLITYKA BEZPIECZEŃSTWA

PRZETWARZANIA DANYCH OSOBOWYCH

„Arntjen Polska Internationale Farmtechnik” Sp. z o.o.

I. POWIĄZANE AKTY PRAWNE

1. **RODO, Rozporządzenie** - Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE;
2. **Ustawa** – Ustawa z dnia 10 maja 2018 roku o ochronie danych osobowych (Dz. U. 2018/1000);
3. **Kodeks pracy** - ustawa z dnia 26 czerwca 1974 r. - Kodeks pracy (tekst jedn.: Dz.U. 2018/917 z późn. zm.).

II. DEFINICJE

- a. **Administrator danych osobowych** – „Arntjen Polska Internationale Farmtechnik” Sp. z o.o. z siedzibą w Paproci, będąca administratorem danych osobowych w rozumieniu art. 4 pkt 7) RODO (dalej **Administrator**);
- b. **Archiwum** – pomieszczenie wyznaczone w budynku siedziby Spółki przeznaczone do przechowywania w uporządkowany sposób zbiorów danych (w tym danych osobowych) w postaci papierowej lub zapisanych na innych fizycznych nośnikach;
- c. **Bezpieczeństwo przetwarzania danych osobowych** - stan, w którym zapewniona jest poufność, autentyczność, dostępność, oraz integralność danych osobowych oraz wyeliminowane lub ograniczone jest prawdopodobieństwo przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do przetwarzanych danych osobowych w stopniu uwzględniającym charakter, zakres, kontekst, cel przetwarzania i ryzyko naruszenia praw lub wolności osób, których dane dotyczą;
- d. **Dane osobowe** – wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
- e. **Dane zwykłe** – dane osobowe nie należące do Szczególnych kategorii danych osobowych;
- f. **Instrukcja zarządzania systemem informatycznym (IZSI)** – przyjęta i obowiązująca w Spółce instrukcja, określająca zasady i procedury zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Spółce;
- g. **Polityka bezpieczeństwa** – niniejsza Polityka bezpieczeństwa przetwarzania danych osobowych zgromadzonych w Spółce;
- h. **Naruszenie, incydent** – naruszenie bezpieczeństwa ochrony danych prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;
- i. **Osoba upoważniona** – osoba posiadająca formalne upoważnienie wydane przez Administratora danych osobowych uprawniona do przetwarzania danych osobowych;
- j. **Podmiot przetwarzający, procesor** – podmiot, któremu Spółka jako administrator danych osobowych zleciła przetwarzanie danych w swoim imieniu;

- k. **Przetwarzanie danych osobowych** – jakiejkolwiek operacje lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takie jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
- l. **Pseudonimizacja** – przetwarzanie danych osobowych w taki sposób, aby nie można było ich przypisać do konkretnej osoby bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno;
- m. **PUODO** – Prezes Urzędu Ochrony Danych Osobowych w Warszawie, ul. Stawki 2; polski organ nadzorczy w rozumieniu RODO;
- n. **Spółka** – „Arntjen Polska Internationale Farmtechnik” Sp. z o.o. z siedzibą w Paproci, zarejestrowana w Sądzie Rejonowym Poznań – Nowe Miasto i Wilda w Poznaniu pod numerem KRS 0000541174, NIP 7792429750;
- o. **Szczególne kategorie danych osobowych** – dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, biometryczne, dotyczące zdrowia, seksualności lub orientacji seksualnej;
- p. **Wytyczne** – wytyczne, zalecenia lub najlepsze praktyki wydawane przez PUODO lub Europejską Radę Ochrony Danych;
- q. **Zbiór danych osobowych** – każdy posiadający strukturę zestaw danych osobowych, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony czy podzielony funkcjonalnie.

III. POSTANOWIENIA OGÓLNE

Niniejsza Polityka bezpieczeństwa określa zasady oraz procedury właściwego zbierania i przetwarzania danych osobowych w „Arntjen Polska Internationale Farmtechnik” Sp. z o.o. w celu zapewnienia bezpieczeństwa przetwarzania tych danych oraz spełnienia wymogów RODO w zakresie ochrony praw i wolności osób fizycznych w związku z przetwarzaniem ich danych osobowych.

IV. CELE POLITYKI BEZPIECZEŃSTWA PRZETWARZANIA DANYCH

Spółka przyjmuje niniejszą Politykę bezpieczeństwa mając na uwadze, że ma ona służyć osiągnięciu następujących celów:

- 1) zdefiniowaniu ogólnych wymagań i zasad ochrony danych osobowych, które będą podstawą dla wszystkich dokumentów związanych z bezpieczeństwem informacji i ochrony danych osobowych;
- 2) zapewnieniu zgodności z przepisami prawa i innymi wymaganiami wynikającymi z zobowiązań umownych związanych z bezpieczeństwem danych osobowych;
- 3) zapewnianiu ochrony aktywów informacyjnych Spółki;
- 4) określenia odpowiedzialności za bezpieczeństwo przepływu informacji i ochronę danych osobowych;
- 5) zminimalizowaniu ryzyka w obszarze bezpieczeństwa informacji i danych osobowych.

V. ORGANIZACJA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH

1. Do przestrzegania zapisów Polityki bezpieczeństwa oraz innych regulacji dotyczących bezpieczeństwa danych osobowych i informacji zobowiązani są wszyscy pracownicy Spółki oraz inne osoby mające dostęp do zasobów informacyjnych Spółki.
2. Odpowiedzialność za zarządzanie bezpieczeństwem sieci i oprogramowania oraz zasady, na jakich powinno się ono odbywać, określa IZSI.

VI. ZASADY DOSTĘPU DO ZASOBÓW DANYCH OSOBOWYCH

1. Do wykonywania czynności przetwarzania danych osobowych w imieniu Administratora mogą być dopuszczone wyłącznie osoby, które posiadają stosowne upoważnienie oraz zobowiązały się do zachowania poufności.
2. Zakres upoważnienia do przetwarzania danych osobowych jest uzależniony i ograniczony do zasobów (zbiorów danych) i środków przetwarzania niezbędnych do wykonania zadań powierzonych danej osobie.
3. Upoważnienia do przetwarzania danych osobowych udziela Administrator.
4. Przetwarzanie danych osobowych nie objętych zakresem upoważnienia lub w inny sposób niż określony w upoważnieniu jest zakazane.
5. Wykorzystanie danych osobowych zebranych przez Spółkę w innym celu niż wynikający z obowiązków służbowych, w szczególności w interesie własnym osoby upoważnionej do przetwarzania danych osobowych lub osób trzecich, jest zakazane.
6. W razie zakończenia współpracy z osobą upoważnioną do przetwarzania danych osobowych lub cofnięcia takiej osobie upoważnienia, Administrator niezwłocznie blokuje dostęp tej osoby do systemów informatycznych.

VII. OBOWIĄZKI OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH

Każda osoba, która została upoważniona do przetwarzania danych osobowych w imieniu Administratora, jest obowiązana znać i stosować w jak największym możliwym zakresie wszelkie dostępne środki ochrony danych osobowych, a przede wszystkim:

- 1) zapoznać się i przestrzegać niniejszej Polityki bezpieczeństwa, Instrukcji zarządzania systemem informatycznym i innych wewnętrznych regulacji, zasad i standardów obowiązujących w Spółce w zakresie ochrony danych osobowych, odpowiednich przepisów prawa oraz uczestniczyć w organizowanych przez Spółkę szkoleniach;
- 2) przetwarzać dane osobowe udostępnione przez Spółkę wyłącznie zgodnie z otrzymanym upoważnieniem;
- 3) informować Administratora o zmianach mających wpływ na aktualność wydanych upoważnień;
- 4) zachować w tajemnicy udostępnione przez Spółkę dane osobowe i sposoby ich zabezpieczenia również po ustaniu zatrudnienia;
- 5) natychmiast po ustaniu zatrudnienia lub odebraniu upoważnienia zaniechać przetwarzania danych osobowych udostępnionych przez Spółkę;
- 6) zabezpieczać dane osobowe i inne dane przed nieuprawnionym dostępem, nieuzasadnionymi modyfikacjami, zniszczeniem, nielegalnym ujawnieniem lub pozyskaniem,

- 7) informować Administratora o wszelkich stwierdzonych podejrzeniach naruszenia ochrony danych oraz słabościach środków zabezpieczenia danych;
- 8) współpracować z Administratorem w przypadku wystąpienia naruszenia ochrony danych na zasadach określonych w niniejszej Polityce bezpieczeństwa;
- 9) informować Administratora o podejrzeniu, że dane osobowe są przetwarzane niezgodnie z prawem: ustal cel przetwarzania, dane są nadmierne w stosunku do celu przetwarzania, nie istnieje albo przestała istnieć podstawa przetwarzania danych itp.

VIII. REAGOWANIE NA INCYDENTY

1. W razie podejrzenia, że wystąpił incydent związany z bezpieczeństwem danych osobowych każda osoba posiadająca wiedzę lub wątpliwość w tym zakresie, zobowiązana jest niezwłocznie zgłosić ten fakt Administratorowi.
2. Zgłoszenie należy dokonać w szczególności w razie stwierdzenia:
 - nieskuteczności zabezpieczenia,
 - naruszenia oczekiwanej integralności, poufności lub dostępności danych,
 - błędu ludzkiego,
 - niezgodności z niniejszą Polityką bezpieczeństwa lub niezgodności z innymi instrukcjami, zasadami lub standardami przyjętymi w Spółce w zakresie ochrony danych,
 - naruszenia ustaleń dotyczących zabezpieczeń fizycznych (np. niezamknięcie pomieszczeń),
 - nienadzorowanych zmian systemu informatycznego,
 - niepoprawnego funkcjonowania sprzętu lub oprogramowania,
 - nieuprawnionego dostępu do zbiorów danych,
 - awarii,
 - kradzieży lub zagubienia nośników danych.
3. W zgłoszeniu należy podać: nazwę systemu informatycznego lub zbioru danych przetwarzanych poza systemem informatycznym oraz powiadomić o zaobserwowanych anomaliach takich jak: rodzaj niezgodności, występujących uszkodzeniach, komunikatach na ekranie.
4. Administrator wydaje osobie zgłaszającej incydent odpowiednie instrukcje postępowania w celu ograniczenia ewentualnych negatywnych skutków naruszenia i w miarę potrzeby udziela pomocy w ich wdrożeniu.
5. Dopuszczalne jest podejmowanie jedynie działań skoordynowanych z Administratorem.
6. Administrator odpowiada za poszukiwanie, zgromadzenie i udokumentowanie wszelkich okoliczności naruszenia i jego zgłoszenia, w tym skutków naruszenia i podjętych działań zaradczych, na potrzeby ewentualnego zgłoszenia naruszenia do PUODO, postępowania dyscyplinarnego lub postępowań sądowych. Dokumentowanie naruszeń odbywa się przy wykorzystaniu rejestru naruszeń.
7. W przypadku stwierdzenia wystąpienia incydentu Administrator lub upoważniona przez niego osoba podejmują czynności w celu:
 - ustalenie czasu zdarzenia będącego incydem,
 - ustalenie zakresu incydentu,

- określenie przyczyn, skutków oraz szacowanych zaistniałych szkód,
 - zabezpieczenie dowodów,
 - ustalenie osób odpowiedzialnych za naruszenie,
 - usunięcie skutków incydentu,
 - ograniczenie szkód wywołanych incydemem,
 - zainicjowanie działań dyscyplinarnych,
 - zarekomendowanie działań zapobiegawczych w kierunku wyeliminowania podobnych zagrożeń w przyszłości,
 - udokumentowanie prowadzonego postępowania w rejestrze naruszeń.
8. Administrator dokonuje oceny charakteru tego naruszenia pod kątem prawdopodobieństwa wywołania skutków w postaci ryzyka naruszenia praw lub wolności osób fizycznych, których dane dotyczą i konieczności zgłoszenia naruszenia do PUODO.

IX. ZASADY PRZETWARZANIA DANYCH OSOBOWYCH POZA SYSTEMAMI INFOMATYCZNYMI

1. Dane w postaci papierowej powinny być przechowywane w sposób zabezpieczający je przed nieuprawnionym ujawnieniem lub zniszczeniem.
2. Zbiory danych w postaci papierowej należy przechowywać w zamkniętych szafach.
3. Pracownicy obowiązani są stosować zasadę czystego biurka, polegającą na tym, że:
 - w trakcie pracy na biurku znajdują się wyłącznie dokumenty niezbędne do wykonywania pracy;
 - przed każdorazowym opuszczeniem stanowiska pracy dokumenty obejmujące dane osobowe są zabezpieczane przed ich ujawnieniem osobom nieuprawnionym;
 - po zakończeniu pracy wszystkie dokumenty i nośniki są zabezpieczane w sposób uniemożliwiający dostęp osób nieuprawnionych.
4. Należy niezwłocznie zabierać wydruki z kopiarek i drukarek, do których dostęp mają osoby zatrudnione w różnych działach lub osoby nieupoważnione do przetwarzania danych. Zabronione jest pozostawianie niepotrzebnych kopii lub wydruków (np. nadmiarowych lub o słabej jakości) w pobliżu urządzeń kopiujących lub drukujących. Dokumenty te należy zawsze niezwłocznie zniszczyć. W razie awarii lub zakłócenia pracy drukarki skutkującego niemożnością niezwłocznego uzyskania wydruku, należy usunąć polecenie drukowania z pamięci urządzenia.
5. Niszczanie dokumentów obejmujących dane osobowe odbywa się w sposób zabezpieczający dane osobowe przed nieuprawnionym ujawnieniem.
6. Zbiory danych powinny być regularnie przeglądane pod kątem upływu okresów przetwarzania. Dokumenty zawierające dane osobowe, których cel przetwarzania odpadł i dane te nie są już niezbędne do jego osiągnięcia, podlegają usunięciu.
7. Należy zachować ostrożność przy ujawnianiu danych osobowych w trakcie rozmów osobistych i telefonicznych, w szczególności prowadzonych w miejscach publicznych, w otwartych biurach, w salach konferencyjnych lub innych miejscach, w których zachodzi ryzyko usłyszenia tych rozmów przez osoby nieuprawnione.
8. Zasady postępowania ze zbiorami danych zapisanymi na wymiennych nośnikach określa IZSI.

X. INFORMATYCZNE ŚRODKI OCHRONY DANYCH

Informatyczne środki ochrony danych określa IZSI.

XI. ORGANIZACJA ARCHIWUM

1. Na terenie siedziby Spółki zorganizowane jest Archiwum.
2. Regały w Archiwum są oznaczone.
3. W Archiwum:
 - przechowuje się akta, które nie są już potrzebne do bieżącej pracy, a zgodnie z obowiązującymi przepisami prawa lub przepisami wewnętrznymi Spółki muszą jeszcze przez określony czas być gromadzone w Spółce;
 - udostępnia się akta dla celów służbowych.
4. Za obsługę Archiwum odpowiedzialny jest wyznaczony przez Dyрекcję pracownik (dalej: Opiekun Archiwum).
5. Archiwum jest zorganizowane w taki sposób, by zabezpieczyć przechowywane tam akta przed uszkodzeniem, zniszczeniem oraz utratą, w szczególności przez zastosowanie takich środków jak:
 - zamontowanie ognioodpornych szaf,
 - zapewnienie skutecznej wentylacji oraz sprawnej instalacji elektrycznej w pomieszczeniach Archiwum,
 - zainstalowanie przeciwpożarowej instalacji sygnalizacyjno-alarmowej,
 - zamieszczenie w Archiwum podręcznego sprzętu gaśniczego,
 - zamykanie Archiwum na klucz.
6. Dokumentacja przekazywana do Archiwum musi być odpowiednio sklasyfikowana i zabezpieczona.
7. Przekazanie dokumentacji jest odnotowywane w ewidencji akt. Ewidencja akt prowadzona jest przez Opiekuna Archiwum w wersji elektronicznej.
8. Wstęp do Archiwum jest możliwy tylko w obecności Opiekuna Archiwum.
9. Dokumenty z Archiwum wydawane są tylko w obecności Opiekuna Archiwum.
10. Zabrania się wnoszenia akt poza teren Zakładu.
11. Klucze do archiwum posiada Opiekun Archiwum oraz Dyrektor Spółki.
12. W przypadku stwierdzenia utraty dokumentacji przechowywanej w Archiwum, włamania do pomieszczeń Archiwum, ich zalania lub zniszczenia w inny sposób Opiekun Archiwum powiadamia niezwłocznie Dyrektora Spółki.
13. Nie rzadziej niż raz w roku archiwizowana dokumentacja podlega przeglądowi pod kątem upływu okresów przetwarzania. Przeglądu dokonuje Opiekun Archiwum. Dokumenty zawierające dane osobowe, których cel przetwarzania odpadł i dane te nie są już niezbędne do jego osiągnięcia, podlegają usunięciu.

XII. ZASADY UDOSTĘPNIANIA DANYCH OSOBOWYCH INNYM PODMIOTOM

- a. Spółka może powierzyć przetwarzanie danych osobowych w swoim imieniu innemu podmiotowi wyłącznie na zasadach określonych w RODO.

- b. Powierzenie przetwarzania danych osobowych może nastąpić po zawarciu umowy regulującej co najmniej kwestie, o których mowa w art. 28 ust. 3 RODO.
- c. Przed zawarciem jakiegokolwiek umowy z kontrahentem zewnętrznym konieczne jest przeprowadzenie analizy, czy w związku z jej wykonaniem nie dojdzie do powierzenia przetwarzania danych osobowych.
- d. W razie ustalenia, że w związku z wykonaniem planowanej umowy nie dojdzie do powierzenia przetwarzania danych osobowych, lecz Spółka będzie udostępniać kontrahentowi dane osobowe, których jest administratorem, konieczne jest przeprowadzenie dalszej analizy, czy wskazane jest zobowiązanie kontrahenta do zachowania poufności danych.

XIII. POSTANOWIENIA KOŃCOWE

1. W sprawach nieuregulowanych w niniejszej Polityce bezpieczeństwa mają zastosowanie przepisy RODO oraz Ustawy oraz przepisów szczególnych.
2. Osoby upoważnione są zobowiązane do bezwzględnego stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Polityce; w wypadku odrębnych od zawartych w niniejszej Polityce uregulowań występujących w innych procedurach obowiązujących w Spółce, osoby upoważnione mają obowiązek stosowania zapisów dalej idących, których stosowanie zapewni wyższy poziom ochrony danych osobowych.
3. Polityka bezpieczeństwa przetwarzania danych osobowych obowiązuje od 07.01.2019 roku.