

POLITYKA OCHRONY DANYCH OSOBOWYCH

1. Postanowienia ogólne

- Niniejsza Polityka Ochrony Danych Osobowych (dalej: „Polityka”) określa zasady przetwarzania danych osobowych w SERPOL COSMETICS Patrycja Serwatka Sp.k z siedzibą w Mieścisku , ul. Nowa 2 ,62-290,
- Polityka została opracowana zgodnie z: Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. (RODO), przepisami prawa krajowego tj. ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych oraz innymi właściwymi przepisami prawa.
- Polityka została zatwierdzona przez Administratora Danych Osobowych i obowiązuje wszystkich pracowników oraz współpracowników.

2. Administrator danych osobowych

- Administratorem danych osobowych jest: SERPOL COSMETICS Patrycja Serwatka Sp.k z siedzibą w Mieścisku , ul. Nowa 2 ,62-290, NIP: 7661985999; Regon: 301798315, KRS 0000391154, Sąd Rejonowy Poznań - Nowe Miasto i Wilda w Poznaniu, IX Wydział Gospodarczy KRS, nr telefonu 61 427-80-79, fax. 61 427-78-01, adres email: biuro@serpol-cosmetics.pl
- Inspektor Ochrony Danych: Kontakt w sprawach dotyczących ochrony danych osobowych: Marcin Piechocki, telefon: +48 512 129 072, e-mail: marcin.piechocki@serpol-cosmetics.pl

3. Zakres stosowania

- Polityka ma zastosowanie do wszystkich pracowników, współpracowników, zleceniobiorców, kandydatów do pracy, przedstawicieli kontrahentów (np. handlowcy, kupcy, logistycy), dostawców będący osobami fizycznymi, goście zakładu (rejstry wejść), praktykantów / stażystów oraz innych osób, które przetwarzają dane osobowe na rzecz Administratora (szczegóły w klauzulach informacyjnych). Polityka stanowi dokument nadrzędny w systemie zarządzania ochroną danych osobowych w Spółce.

4. Zasady ochrony danych osobowych

Administrator zapewnia przetwarzanie danych osobowych zgodnie z zasadami art. 5 RODO:

- legalności, rzetelności i przejrzystości - dane są przetwarzane zgodnie z prawem, uczciwie i w sposób zrozumiały zgodnie z klauzulami informacyjnymi RODO.
- ograniczenia celu - zbieramy dane tylko w konkretnym celu i nie używamy ich do czegoś innego.
- minimalizacji danych - zbieramy tylko tyle danych, ile naprawdę potrzebujemy.
- Prawidłowości - dane są aktualne i poprawne, a w przypadku wniosku pracownika o zmianę aktualizowane zgodnie z zapisami zawartymi we wniosku.
- ograniczenia przechowywania - nie trzymamy danych dłużej niż trzeba zgodnie z przepisami prawa lub wewnętrznymi procedurami.
- integralności i poufności - dane są zabezpieczone przed utratą, zniszczeniem i dostępem osób nieuprawnionych.
- rozliczalności – jesteśmy w stanie udowodnić, że spełniamy wszystkie powyższe zasady prowadzoną dokumentacją, polityki, rejestry, procedury oraz wykazanie dowodów na zgodność.

5. Kategorie danych osobowych

Przetwarzane mogą być w szczególności: imię i nazwisko, dane kontaktowe (numer telefonu, adres e-mail), dane identyfikacyjne (PESEL), adres zamieszkania, dane kadrowo-płacowe, dane zawarte w umowach, orzeczenia medycyny pracy oraz dane związane z bezpieczeństwem (monitoring wizyjny, kontrola dostępu). Szczegółowe zapisy kategorii zawarte są w Rejestrze Czynności Przetwarzania.

6. Cele przetwarzania

Dane osobowe są przetwarzane w następujących celach: realizacja stosunku pracy i obowiązków pracodawcy, prowadzenie procesów rekrutacyjnych, realizacja umów z kontrahentami i dostawcami, kontakt operacyjny, techniczny i handlowy, realizacja obowiązków prawnych i księgowych, zapewnienie bezpieczeństwa zakładu produkcyjnego oraz ochrony mienia. Szczegółowe cele wraz z podstawami prawnymi zawarte zostały w klauzulach informacyjnych RODO.

7. Podstawy prawne przetwarzania danych

Dane osobowe są przetwarzane na podstawie:

- art. 6 ust. 1 lit. a RODO – zgoda kandydata na udział w przyszłych rekrutacjach
- art. 6 ust. 1 lit. b RODO – przetwarzanie niezbędne do realizacji umowy o pracę, działań przed jej zawarciem, porozumienia, umowy o praktykę,
- art. 6 ust. 1 lit. c RODO – obowiązki prawne administratora w zakresie danych wymaganych przepisami prawa pracy, przetwarzanie niezbędne do wypełnienia obowiązków prawnych ciążących na administratorze (w szczególności w zakresie BHP), obowiązki prawne administratora (prawo podatkowe i rachunkowe),
- art. 6 ust. 1 lit. f RODO – prawnie uzasadniony interes administratora w związku z art. 22.2 KP , prawnie uzasadniony interes administratora polegający na sprawnej i bezpiecznej realizacji procesu dostawy towarów, prawnie uzasadniony interes administratora (kontakt biznesowy, dochodzenie roszczeń), prawnie uzasadniony interes administratora polegający na utrzymywaniu relacji biznesowych, prawnie uzasadniony interes administratora polegający na obsłudze zapytań kierowanych do firmy za pomocą strony internetowej.
- art. 9 ust. 2 lit. b RODO – dane dotyczące zdrowia (medycyna pracy), przetwarzanie danych szczególnych kategorii (dotyczących zdrowia) w związku z obowiązkami z zakresu prawa pracy i bezpieczeństwa pracy (orzeczenie lekarza medycyny pracy),

8. Odbiorcami danych osobowych mogą być: firmy księgowe i kadrowo-płacowe, dostawy usług IT i systemów ERP/HR, firmy ochroniarskie, kancelarie prawne, organy publiczne (ZUS, US, PIP) – na podstawie przepisów prawa. Przekazywanie danych odbywa się na podstawie umów powierzenia przetwarzania danych.

9. Przekazywanie danych poza UE/EOG

Dane osobowe nie są przekazywane poza UE/EOG.

10. Okres przechowywania danych

Dane osobowe są przechowywane przez okres niezbędny do realizacji celów określonych powyżej na czas wykonania umowy, okres, na jaki obligują Administratora przepisy prawa, do czasu przedawnienia ewentualnych roszczeń lub do czasu wycofania zgody tj, dokumentacja pracownicza – zgodnie z KP, monitoring – maksymalnie 3 miesiące, dane kandydatów – do zakończenia rekrutacji, dokumentacja księgowa - okres wymagany przepisami prawa podatkowego i rachunkowego 5 lat.

11. Zarządzanie upoważnieniami do przetwarzania danych

Administrator zapewnia, że dostęp do danych osobowych posiadają wyłącznie osoby upoważnione, w zakresie niezbędnym do realizacji powierzonych im obowiązków służbowych. Upoważnienia do przetwarzania danych osobowych są nadawane, modyfikowane i odbierane w sposób kontrolowany, zgodnie z obowiązującymi w Spółce procedurami oraz zasadą minimalizacji dostępu. Każda osoba przetwarzająca dane osobowe zobowiązana jest do zachowania poufności zarówno w trakcie trwania współpracy, jak i po jej zakończeniu. Administrator prowadzi ewidencję nadanych upoważnień oraz regularnie weryfikuje ich aktualność i zasadność.

12. Prawa osób, których dane dotyczą

Każda osoba ma prawo do:

- Art. 15 – Prawo dostępu do danych
- Art. 16 – Prawo do sprostowania
- Art. 17 – Prawo do usunięcia („prawo do bycia zapomnianym”) poza danymi, których usunięcie reguluje obowiązek prawny
- Art. 18 – Prawo do ograniczenia przetwarzania
- Art. 19 – Obowiązek informowania o zmianach
- Art. 20 – Prawo do przenoszenia danych
- Art. 21 – Prawo do sprzeciwu
- Art. 22 – Decyzje automatyczne (profilowanie)
- Art. 77 - prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych w przypadku przetwarzania niezgodnego z przepisami RODO.

13. Obowiązki pracowników:

- Przetwarzanie danych tylko zgodnie z poleceniem na podstawie upoważnienia
- Zachowanie poufności - nie ujawnianie danych osobom nieuprawnionym w firmie (innym działom bez potrzeby) oraz poza firmą (rodzina, znajomi)
- Zabezpieczanie danych - dbanie o bezpieczeństwo (w praktyce: blokowanie komputera, nie udostępnianie haseł, nie zostawianie dokumentów na widoku (clean desk))
- Minimalizacja danych - korzystanie tylko z tych danych, które są potrzebne (
- Zgłaszanie incydentów w przypadku ujawnienia danych osobom nieuprawnionym (np. wysyłka maila do złej osoby) → zgłoszenie od razu bez zbędnej zwłoki
- Przestrzeganie procedur - stosowanie polityki firmy: bezpieczeństwa informacji, ochrony danych, korzystania z systemów IT
- Aktualność i poprawność danych w przypadku wykrycia błędu → zgłaszanie lub poprawianie błędów

14. Środki bezpieczeństwa

Dbamy o bezpieczeństwo danych osobowych, stosując różne zabezpieczenia, m.in.:

- Środki organizacyjne (czyli zasady i procedury) → polityka ochrony danych i bezpieczeństwa informacji, nadawanie i odbieranie uprawnień (kto ma dostęp do czego), szkolenia pracowników z RODO, upoważnienia do przetwarzania danych, zasady zgłaszania incydentów, backupów, udostępniania danych
- Środki techniczne (czyli IT i zabezpieczenia) → narzędzia i systemy tj. hasła i uwierzytelnianie (np. MFA), szyfrowanie danych i dysków, zabezpieczenia systemów informatycznych, firewall, antywirus, aktualizacje systemów, kopie zapasowe (backupy), nadawanie dostępu w systemach, logowanie operacji (kto co zrobił), automatyczne blokady komputerów kilku minutach
- Zabezpieczenia fizyczne → „ochrona miejsca, gdzie są dane” tj. zamykane szafy na dokumenty, kontrola dostępu do biura, monitoring, niszczenie dokumentów (niszczarki),

15. Naruszenia ochrony danych osobowych

Naruszenie danych to nieuprawniony dostęp, utrata lub ujawnienie informacji w firmie produkcyjnej lub magazynowej np. zgubiona lista, wysłany e-mail do złej osoby, pozostawione dokumenty, nieuprawniony dostęp, zdjęcie dokumentu, prywatny telefon, zdjęcie pulpitu zawierające dane wysłane w mailu.

Praktyczny schemat działania:

wykryj → zgłoś → zabezpiecz → oceń → (ew. zgłoś do UODO i poinformuj osoby) → udokumentuj → popraw system

- Identyfikacja naruszenia → czyli: co się stało? (mail z danymi wysłany do złej osoby, zgubiony laptop / pendrive, wyciek danych z systemu, dostęp osoby nieuprawnionej)
- Zgłoszenie incydentu wewnętrznie (natychmiast) → pracownik → przełożony / IT / IOD

- **Zabezpieczenie sytuacji (ograniczenie skutków) → szybkie działania techniczne i organizacyjne: cofnięcie dostępu, zmiana haseł, próba cofnięcia maila, kontakt z nieuprawnionym odbiorcą, zablokowanie systemu**
- **Ocena ryzyko dla osób → najważniejsze pytanie: Czy naruszenie może zaszkodzić osobom? (np.: kradzież tożsamości, straty finansowe, utrata prywatności).**
- **Zgłoszenie do organu nadzorczego → jeśli ryzyko istnieje → zgłoszenie do Urząd Ochrony Danych Osobowych maksymalnie 72 godziny od wykrycia (zgłoszenie zawiera m.in.: co się stało, jakie dane, ilu osób dotyczy, jakie działania podjęte). Poinformowanie osób, których dane dotyczą jeśli ryzyko jest wysokie: informujesz bezpośrednio osoby, jasno: co się stało i co mogą .**
- **Dokumentacja naruszenia nawet jeśli nie zostało zgłoszone do UODO (opis zdarzenia, skutki, podjęte działania**
- **Działania naprawcze żeby sytuacja się nie powtórzyła: zmiana procedur, dodatkowe szkolenia, poprawa zabezpieczeń**

16. Privacy by design i privacy by default

Spółka wdraża ochronę danych:

- **już na etapie projektowania procesów (privacy by design),**
- **w ustawieniach domyślnych systemów i procedur (privacy by default), z uwzględnieniem charakteru, zakresu i ryzyka przetwarzania.**

17. Postanowienia końcowe

Polityka podlega okresowym corocznym przeglądom, aktualizacji w przypadku zmian prawa lub procesów oraz zatwierdzeniu przez Administratora Danych Osobowych. Dokument jest dostępny dla pracowników i współpracowników Administratora.

18. Dokumentacja i zgodność

System ochrony danych osobowych w Spółce obejmuje niniejszą Politykę, Procedurę Ochrony Danych Osobowych, rejestry RCP, rejestr umów powierzenia.