PIEROŃCZYK
SUBCONTRACTING PRECISION PRODUCTS
KOLEJNICTWO · PRZEMYSŁ · MOTORYZACJA

Ślusarstwo Produkcyjne
inż. Andrzej Pierończyk
ul. Budowlana 5, 41-100 Siemianowice Śląskie
NIP 6430003808 · REGON 270579373 · BDO 000245386
ING Bank Śląski PLN: 25 1050 1214 1000 0007 0041 2505
ING Bank Śląski EUR: PL68 1050 1214 1000 0090 7094 9616 · SWIFT/BIC: INGBPLPW

POLITYKA OCHRONY DANYCH OSOBOWYCH I BEZPIECZEŃSTWA INFORMACJI

SUBCONTRACTING PRECISION PRODUCTS

Dokument	Polityka ochrony danych osobowych i bezpieczeństwa informacji
Wersja	1.0
Data wprowadzenia	2026-06-30
Obowiązuje od	2026-07-01
Status	Dokument wewnętrzny / firmowy

Niniejszy dokument określa zasady ochrony danych osobowych oraz bezpieczeństwa informacji w Ślusarstwie Produkcyjnym inż. Andrzej Pierończyk. Dokument obejmuje całą organizację: pracowników, współpracowników, rekrutację, kontrahentów, dostawców, gości, dokumentację techniczną, korespondencję, systemy IT, archiwum, stronę internetową, monitoring, kopie zapasowe oraz nośniki danych.

Uwaga wdrożeniowa: pola oznaczone jako "do uzupełnienia" należy wypełnić rzeczywistymi nazwami systemów, dostawców usług, lokalizacji danych, okresów retencji i osób odpowiedzialnych przed zatwierdzeniem dokumentu.

SPIS TREŚCI

1. Cel dokumentu, zakres i odpowiedzialność
2. Kategorie osób, danych i procesów przetwarzania
3. Zasady ochrony danych osobowych
4. Organizacja bezpieczeństwa informacji
5. Upoważnienia, poufność i szkolenia
6. Rejestr czynności, obowiązki informacyjne i prawa osób
7. Retencja, archiwizacja, podmioty przetwarzające i transfery
8. Naruszenia, ocena ryzyka, DPIA i privacy by design
9. Monitoring, kontrola dostępu i dane gości
10. Przeglądy i postanowienia końcowe
Załącznik 1. Rejestr czynności przetwarzania danych
Załącznik 2. Wykaz procesorów, odbiorców i umów powierzenia
Załącznik 3. Tabela retencji i usuwania danych
Załącznik 4. Procedura i rejestr żądań osób, których dane dotyczą
Załącznik 5. Procedura naruszeń, formularz i matryca decyzji
Załącznik 6. Upoważnienia, ewidencja osób upoważnionych i poufność
Załącznik 7. Wykaz ról i odpowiedzialności
Załącznik 8. Minimalne wymagania bezpieczeństwa IT
Załącznik 9. Ocena ryzyka i DPIA - lista kontrolna
Załącznik 10. Klauzule informacyjne
Załącznik 11. Potwierdzenie zapoznania z Polityką

Ślusarstwo Produkcyjne
inż. Andrzej Pierończyk
ul. Budowlana 5, 41-100 Siemianowice Śląskie
NIP 6430003808 · REGON 270579373 · BDO 000245386
ING Bank Śląski PLN: 25 1050 1214 1000 0007 0041 2505
ING Bank Śląski EUR: PL68 1050 1214 1000 0090 7094 9616 · SWIFT/BIC: INGBPLPW

ROZDZIAŁ I. CEL DOKUMENTU, ZAKRES I ODPOWIEDZIALNOŚĆ

§ 1. Cel polityki

Celem Polityki jest zapewnienie zgodnego z prawem, kontrolowanego i rozliczalnego przetwarzania danych osobowych w SPP (Ślusarstwo Produkcyjne inż. Andrzej Pierończyk) oraz wykazanie rozliczalności Administratora. Polityka jest dokumentem nadrzędnym wobec szczegółowych instrukcji, rejestrów i formularzy dotyczących ochrony danych, bezpieczeństwa informacji oraz organizacji pracy z dokumentami.

Politykę stosuje się w procesach produkcyjnych i administracyjnych zakładu, w szczególności przy obsłudze klientów przemysłowych, przygotowaniu ofert, analizie dokumentacji technicznej, realizacji zamówień, kontroli jakości, logistyce, zakupach, księgowości, kadrach, rekrutacji, współpracy z dostawcami i podwykonawcami oraz obsłudze gości.

§ 2. Administrator danych

Administratorem danych osobowych jest Ślusarstwo Produkcyjne inż. Andrzej Pierończyk, ul. Budowlana 5, 41-100 Siemianowice Śląskie, NIP 6430003808, REGON 270579373, BDO 000245386, e-mail: biuro@pieronczyk.pl. Administrator ustala cele i sposoby przetwarzania danych oraz odpowiada za wdrożenie środków organizacyjnych i technicznych adekwatnych do ryzyka.

§ 3. Zakres podmiotowy

Polityka obowiązuje wszystkie osoby, które przetwarzają dane w imieniu lub na rzecz Administratora, niezależnie od podstawy współpracy, w tym:

- właściciela, osoby zarządzające i osoby upoważnione do reprezentowania firmy;
- pracowników, zleceniobiorców, współpracowników B2B, praktykantów i stażystów;
- osoby prowadzące rekrutację, kadry, księgowość, administrację, zakupy, sprzedaż, logistykę, jakość, produkcję i utrzymanie ruchu;
- podwykonawców, serwisantów, dostawców usług IT, księgowych, prawnych, kadrowych i innych podmiotów przetwarzających dane;
- gości, audytorów, przedstawicieli klientów i dostawców przebywających na terenie zakładu.

§ 4. Inspektor ochrony danych

Na dzień przygotowania niniejszej wersji Polityki dokument zakłada, że Administrator nie powołuje Inspektora Ochrony Danych, chyba że odrębna ocena wykaże obowiązek lub celowość jego powołania. Ocena przesłanek powołania IOD powinna być dokonywana co najmniej raz w roku oraz po istotnej zmianie skali lub charakteru przetwarzania danych. Na dzień zatwierdzenia Polityki Administrator nie spełnia przesłanek obowiązkowego powołania IOD z art. 37 ust. 1 RODO: podstawowa działalność SPP nie polega na operacjach przetwarzania wymagających regularnego i systematycznego monitorowania osób na dużą skalę ani na przetwarzaniu na dużą skalę danych szczególnych kategorii. Decyzję o niepowoływaniu IOD wraz z uzasadnieniem dokumentuje Administrator.

ROZDZIAŁ II. KATEGORIE OSÓB, DANYCH I PROCESÓW PRZETWARZANIA

§ 5. Kategorie osób

- kandydaci do pracy, pracownicy, byli pracownicy oraz członkowie rodzin pracowników w zakresie wymaganym prawem pracy i ubezpieczeń społecznych;
- współpracownicy, zleceniobiorcy, podwykonawcy i osoby działające w imieniu kontrahentów;
- przedstawiciele klientów, dostawców, partnerów biznesowych, jednostek certyfikujących, audytorów, przewoźników i serwisów technicznych;
- goście zakładu, osoby zgłaszające wizytę, uczestnicy spotkań i osoby przekazujące rysunki techniczne lub zapytania ofertowe;
- osoby kontaktujące się przez e-mail, telefon, stronę internetową lub korespondencję tradycyjną;
- osoby utrwalone przez monitoring wizyjny, jeżeli przebywają w strefach monitorowanych.

§ 6. Kategorie danych

- dane identyfikacyjne i kontaktowe: imię, nazwisko, stanowisko, firma, adres e-mail, numer telefonu, adres korespondencyjny;
- dane kadrowe: PESEL, data urodzenia, adres, dokumenty zatrudnienia, kwalifikacje, szkolenia BHP, uprawnienia, badania lekarskie, wynagrodzenia, urlopy, dokumentacja ZUS i podatkowa;
- dane rekrutacyjne: CV, kwalifikacje, uprawnienia, doświadczenie i dane kontaktowe;
- dane kontraktowe i księgowe: dane osób reprezentujących kontrahenta, zamówienia, faktury, umowy i korespondencja;
- dane techniczne i jakościowe: dane osób uczestniczących w korespondencji projektowej, zatwierdzeniach, audytach, odbiorach i reklamacjach;
- dane IT: loginy, identyfikatory użytkowników, logi systemowe, adresy IP, historia dostępu i zmian;
- dane gości i bezpieczeństwa zakładu: imię, nazwisko, firma, cel wizyty, osoba odwiedzana, czas wejścia i wyjścia, ewentualnie numer pojazdu i wizerunek przy monitoringu.

§ 7. Dane szczególnych kategorii i dane karne

Dane szczególnych kategorii, w szczególności dane o zdrowiu, mogą być przetwarzane wyłącznie w zakresie wynikającym z przepisów prawa pracy, BHP, medycyny pracy, ubezpieczeń społecznych lub w innych prawnie dopuszczalnych przypadkach.

Ślusarstwo Produkcyjne
inż. Andrzej Pierończyk
ul. Budowlana 5, 41-100 Siemianowice Śląskie
NIP 6430003808 · REGON 270579373 · BDO 000245386
ING Bank Śląski PLN: 25 1050 1214 1000 0007 0041 2505
ING Bank Śląski EUR: PL68 1050 1214 1000 0090 7094 9616 · SWIFT/BIC: INGBPLPW

Dane dotyczące wyroków skazujących i naruszeń prawa nie są przetwarzane, chyba że konkretny przepis prawa pozwala lub nakazuje ich pozyskanie.

ROZDZIAŁ III. ZASADY OCHRONY DANYCH OSOBOWYCH

§ 8. Zasady podstawowe

Administrator i osoby upoważnione stosują zasady: legalności, rzetelności i przejrzystości; ograniczenia celu; minimalizacji danych; prawidłowości; ograniczenia przechowywania; integralności i poufności oraz rozliczalności. Każdy proces powinien mieć zidentyfikowany cel, podstawę prawną, zakres danych, odbiorców, retencję i środki bezpieczeństwa.

§ 9. Podstawy przetwarzania

- niezbędność do zawarcia lub wykonania umowy, w tym umowy o pracę, umowy handlowej, zamówienia lub umowy z podwykonawcą;
- obowiązek prawny z zakresu prawa pracy, podatków, rachunkowości, BHP, ubezpieczeń społecznych i archiwizacji;
- prawnie uzasadniony interes Administratora, np. kontakt z przedstawicielami kontrahentów, dochodzenie roszczeń, zapewnienie bezpieczeństwa zakładu, ochrona mienia i prowadzenie korespondencji;
- zgoda osoby, której dane dotyczą, gdy przepisy wymagają zgody lub gdy dane są przetwarzane poza podstawowym celem;
- ochrona żywotnych interesów osoby fizycznej w wyjątkowych sytuacjach zagrożenia życia lub zdrowia.

§ 10. Zakaz nieuzasadnionego kopiowania dokumentów

Nie kopiuje się dowodów osobistych, praw jazdy, paszportów, legitymacji, kart płatniczych, dokumentacji medycznej lub dokumentów zawierających dane szczególnych kategorii, jeżeli nie wynika to wprost z przepisu prawa lub udokumentowanej potrzeby. Jeżeli wystarczające jest potwierdzenie informacji, należy odnotować fakt weryfikacji bez utrwalania całego dokumentu.

ROZDZIAŁ IV. ORGANIZACJA BEZPIECZEŃSTWA INFORMACJI

§ 11. Bezpieczeństwo organizacyjne

- dostęp do danych nadaje się zgodnie z zasadą wiedzy koniecznej;
- dostęp do systemów i zasobów jest imienny i nie może być współdzielony;
- dokumenty zawierające dane osobowe przechowuje się w miejscach zabezpieczonych przed dostępem osób nieuprawnionych;
- wydruki, notatki, dokumentacja techniczna i nośniki danych nie mogą pozostawać bez nadzoru w miejscach ogólnodostępnych;
- dane przesyłane elektronicznie zabezpiecza się adekwatnie do ich wrażliwości, np. hasłem, szyfrowaniem, ograniczeniem odbiorców lub osobnym przekazaniem hasła;
- dostęp osób zewnętrznych do pomieszczeń, systemów lub dokumentacji odbywa się tylko w zakresie niezbędnym i pod nadzorem osoby odpowiedzialnej.

§ 12. Bezpieczeństwo techniczne i IT

Systemy informatyczne, poczta elektroniczna, dyski sieciowe, komputery, laptopy, urządzenia mobilne, maszyny z interfejsami sieciowymi oraz nośniki zewnętrzne powinny być zabezpieczone zgodnie z minimalnymi wymaganiami IT określonymi w Załączniku 8. Kopie zapasowe powinny obejmować dane istotne dla ciągłości działania, w tym dokumentację handlową, kadrową, księgową, techniczną i jakościową. Administrator lub wyznaczona osoba okresowo weryfikuje, czy kopie są wykonywane i możliwe do odtworzenia.

§ 13. Dokumentacja techniczna i dane klientów

Rysunki techniczne, modele, zapytania ofertowe, dokumentacja produkcyjna, dokumenty jakościowe, certyfikaty materiałowe, dokumentacja spawalnicza oraz korespondencja projektowa mogą zawierać dane osobowe pracowników klientów, dostawców, projektantów, audytorów lub osób zatwierdzających dokumentację. Dostęp do dokumentacji przyznaje się wyłącznie osobom uczestniczącym w realizacji danego procesu. Dokumentacji klienta nie przesyła się na prywatne skrzynki e-mail i nie przechowuje na prywatnych urządzeniach.

ROZDZIAŁ V. UPOWAŻNIENIA, POUFNOŚĆ I SZKOLENIA

§ 14. Upoważnienia i ewidencja

Dostęp do danych osobowych może uzyskać wyłącznie osoba upoważniona przez Administratora lub osobę przez niego wskazaną. Upoważnienie określa osobę, stanowisko lub rolę, zakres danych, systemy lub dokumentację, cel dostępu oraz datę nadania i cofnięcia uprawnień. Administrator prowadzi ewidencję osób upoważnionych.

§ 15. Poufność

Każda osoba upoważniona jest zobowiązana do zachowania w poufności danych osobowych, informacji technicznych, handlowych oraz innych informacji nieprzeznaczonych do publicznego ujawnienia. Obowiązek poufności trwa także po ustaniu zatrudnienia lub współpracy.

Ślusarstwo Produkcyjne
inż. Andrzej Pierończyk
ul. Budowlana 5, 41-100 Siemianowice Śląskie
NIP 6430003808 · REGON 270579373 · BDO 000245386
ING Bank Śląski PLN: 25 1050 1214 1000 0007 0041 2505
ING Bank Śląski EUR: PL68 1050 1214 1000 0090 7094 9616 · SWIFT/BIC: INGBPLPW

§ 16. Szkolenia i świadomość

Osoby przetwarzające dane powinny zostać zapoznane z niniejszą Polityką przed uzyskaniem dostępu do danych. Szkolenia lub instruktaż obejmują zasady RODO, poufność, bezpieczeństwo IT, zgłaszanie incydentów, czyste biurko, bezpieczną korespondencję oraz zasady przekazywania dokumentacji technicznej.

ROZDZIAŁ VI. REJESTR CZYNNOŚCI, OBOWIĄZKI INFORMACYJNE I PRAWA OSÓB

§ 17. Rejestr czynności przetwarzania

Administrator prowadzi Rejestr Czynności Przetwarzania Danych zgodnie z Załącznikiem 1. Rejestr obejmuje cele, kategorie osób i danych, podstawy prawne, odbiorców, procesorów, systemy, lokalizacje danych, transfery, okresy usuwania oraz ogólny opis środków bezpieczeństwa. Rejestr aktualizuje się przy wdrożeniu nowego procesu, systemu, dostawcy, istotnej zmianie zakresu danych lub po audycie.

§ 18. Obowiązki informacyjne

Administrator przekazuje osobom, których dane dotyczą, informacje wymagane przez RODO w momencie zbierania danych albo w innym terminie przewidzianym prawem. Klauzule informacyjne stanowią Załącznik 10 i powinny być dostosowane do faktycznego procesu, odbiorców, okresów retencji i stosowanych systemów.

§ 19. Prawa osób i obsługa żądań

Osobom, których dane dotyczą, przysługują prawa określone w RODO, w tym prawo dostępu do danych, sprostowania, usunięcia, ograniczenia przetwarzania, przenoszenia danych, sprzeciwu, cofnięcia zgody oraz wniesienia skargi do organu nadzorczego. Żądania osób przyjmuje właściciel, osoba koordynująca ochronę danych lub osoba wyznaczona do obsługi danego procesu. Procedura i rejestr żądań są określone w Załączniku 4.

ROZDZIAŁ VII. RETENCJA, ARCHIWIZACJA, PODMIOTY PRZETWARZAJĄCE I TRANSFERY

§ 20. Retencja danych

Dane osobowe przechowuje się przez okres wynikający z celu przetwarzania, przepisów prawa, czasu trwania umowy, okresu przedawnienia roszczeń albo uzasadnionej potrzeby dowodowej. Po upływie okresu przechowywania dane należy usunąć, zanonimizować lub przekazać do archiwum zgodnie z zasadami bezpieczeństwa. Szczegółowa tabela retencji stanowi Załącznik 3.

§ 21. Podmioty przetwarzające i udostępnianie danych

Przed dopuszczeniem podmiotu zewnętrznego do danych Administrator ocenia, czy podmiot działa jako procesor, odrębny administrator, współadministrator czy odbiorca danych. Jeżeli podmiot przetwarza dane w imieniu Administratora, należy zawrzeć umowę powierzenia lub zapewnić równoważną podstawę prawną. Wykaz procesorów i odbiorców stanowi Załącznik 2.

§ 22. Transfery poza EOG

Danych osobowych nie przekazuje się poza Europejski Obszar Gospodarczy bez uprzedniej weryfikacji podstawy transferu, zabezpieczeń i dokumentacji wymaganej przez RODO. Dotyczy to w szczególności usług chmurowych, narzędzi poczty elektronicznej, systemów współdzielenia plików, zdalnego wsparcia IT oraz podwykonawców spoza EOG.

ROZDZIAŁ VIII. NARUSZENIA, OCENA RYZYKA, DPIA I PRIVACY BY DESIGN

§ 23. Zgłaszanie incydentów i naruszeń

Każda osoba, która zauważy lub podejrzewa naruszenie ochrony danych, jest zobowiązana niezwłocznie zgłosić zdarzenie właścicielowi, przełożonemu lub osobie koordynującej sprawy ochrony danych. Zgłoszenia dokonuje się niezależnie od tego, czy naruszenie powstało z winy zgłaszającego. Formularz, rejestr i matryca decyzji stanowią Załącznik 5.

§ 24. Ocena i notyfikacja naruszenia

Po otrzymaniu zgłoszenia Administrator ustala fakty, zakres danych, liczbę osób, możliwe skutki, przyczynę zdarzenia i środki zaradcze. Każde naruszenie dokumentuje się, nawet jeśli nie wymaga zgłoszenia organowi nadzorczemu. Jeżeli naruszenie może powodować ryzyko naruszenia praw lub wolności osób fizycznych, Administrator dokonuje zgłoszenia do organu nadzorczego bez zbędnej zwłoki, co do zasady nie później niż w terminie 72 godzin od stwierdzenia naruszenia. Opóźnienie powyżej 72 godzin wymaga pisemnego uzasadnienia.

§ 25. Ocena ryzyka i DPIA

Administrator stosuje podejście oparte na ryzyku. Ocena ryzyka powinna być wykonywana dla nowych systemów, procesów, znaczących zmian organizacyjnych, wdrożenia monitoringu, usług chmurowych, outsourcingu, zdalnego dostępu, przetwarzania danych szczególnych kategorii lub zdarzeń naruszenia. Jeżeli planowany proces może powodować wysokie ryzyko, Administrator przed rozpoczęciem przetwarzania przeprowadza DPIA. Lista kontrolna stanowi Załącznik 9.

Ślusarstwo Produkcyjne
inż. Andrzej Pierończyk
ul. Budowlana 5, 41-100 Siemianowice Śląskie
NIP 6430003808 · REGON 270579373 · BDO 000245386
ING Bank Śląski PLN: 25 1050 1214 1000 0007 0041 2505
ING Bank Śląski EUR: PL68 1050 1214 1000 0090 7094 9616 · SWIFT/BIC: INGBPLPW

§ 26. Privacy by design i privacy by default

Przy projektowaniu nowych procesów, formularzy, umów, rozwiązań IT i organizacji pracy Administrator uwzględnia ochronę danych od początku projektu. Domyślne ustawienia powinny ograniczać zakres zbieranych danych, dostęp, czas przechowywania i liczbę odbiorców do minimum niezbędnego dla celu.

ROZDZIAŁ IX. MONITORING, KONTROLA DOSTĘPU I DANE GOŚCI

§ 27. Goście zakładu

Wejście osób zewnętrznych na teren zakładu może wiązać się z przetwarzaniem danych potrzebnych do bezpieczeństwa, organizacji wizyty, ochrony tajemnicy przedsiębiorstwa, BHP, obsługi audytu lub spotkania. Zakres danych gości powinien być ograniczony do niezbędnego minimum.

§ 28. Monitoring wizyjny

Monitoring wizyjny stosuje się zgodnie z odrębnym dokumentem: Regulamin monitoringu wizyjnego SPP. Publicznie udostępnia się ogólną klauzulę informacyjną i oznakowanie stref monitorowanych. Szczegółowy wykaz kamer, ich lokalizacji, kątów obserwacji i funkcji technicznych jest dokumentem wewnętrznym, nie jest publikowany na stronie internetowej i jest dostępny wyłącznie dla osób upoważnionych, serwisu systemu, audytorów lub organów uprawnionych na podstawie przepisów prawa. SPP nie stosuje monitoringu służbowej poczty elektronicznej, monitoringu aktywności na stanowiskach komputerowych ani monitoringu lokalizacji (GPS) pojazdów. Wprowadzenie którejkolwiek z tych form wymagałoby uprzedniej podstawy, aktualizacji dokumentacji oraz poinformowania pracowników zgodnie z art. 22(3) Kodeksu pracy.

ROZDZIAŁ X. PRZEGLĄDY I POSTANOWIENIA KOŃCOWE

§ 29. Audyty i przeglądy

Administrator dokonuje przeglądu niniejszej Polityki co najmniej raz na 12 miesięcy, a także po istotnej zmianie organizacyjnej, wdrożeniu nowego systemu, zmianie przepisów, stwierdzeniu naruszenia, audycie klienta, zmianie podmiotów przetwarzających lub zmianie zakresu danych przetwarzanych w firmie. Na dzień zatwierdzenia Polityki liczba osób wykonujących pracę na rzecz Administratora nie osiąga progu 50, w związku z czym nie powstaje obowiązek wdrożenia wewnętrznej procedury zgłoszeń nieprawidłowości (sygnaliści) ani obowiązek utworzenia Zakładowego Funduszu Świadczeń Socjalnych; SPP nie prowadzi ZFŚS. Status ten podlega przeglądowi przy wzroście zatrudnienia.

§ 30. Pakiet wdrożeniowy

Na pakiet wdrożeniowy ochrony danych składają się co najmniej: niniejsza Polityka, rejestr czynności, wykaz procesorów, upoważnienia, ewidencja osób upoważnionych, oświadczenia o poufności, rejestr naruszeń, rejestr żądań osób, klauzule informacyjne, regulamin monitoringu, polityka prywatności strony WWW, procedura nadawania i odbierania dostępów IT oraz potwierdzenia zapoznania pracowników z Polityką.

§ 31. Postanowienia końcowe

Polityka wchodzi w życie z dniem zatwierdzenia przez Administratora. Wszelkie odstępstwa od Polityki wymagają zgody Administratora lub osoby przez niego wyznaczonej i powinny zostać udokumentowane, jeżeli mogą wpływać na prawa lub wolności osób fizycznych. Dokument jest dokumentem wewnętrznym Administratora.

Opracował / zweryfikował	Zatwierdził - Administrator / Pracodawca
Signature Not Verified Dokument podpisany przez Damian Grzegorz Pierończyk Data: 2026.06.30 19:14:14 CEST ..... data i podpis	Signature Not Verified Dokument podpisany przez Andrzej Pierończyk Data: 2026.06.30 19:15:21 CEST ..... data i podpis