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

PERSONAL DATA PROTECTION AND INFORMATION SECURITY POLICY

Document	Personal data protection and information security policy
Version	1.0
Date introduced	2026-06-30
In force from	2026-07-01
Status	Internal / company document

This document sets out the principles of personal data protection and information security at Ślusarstwo Produkcyjne inż. Andrzej Pierończyk. It covers the entire organisation: employees, associates, recruitment, contractors, suppliers, guests, technical documentation, correspondence, IT systems, archives, the company website, CCTV monitoring, backups and data carriers.

Implementation note: fields marked "to be completed" should be filled in with the actual names of systems, service providers, data locations, retention periods and responsible persons before the document is approved.

TABLE OF CONTENTS

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

CHAPTER I. PURPOSE, SCOPE AND RESPONSIBILITY

§ 1. Purpose of the policy

The purpose of the Policy is to ensure lawful, controlled and accountable processing of personal data at SPP (Ślusarstwo Produkcyjne inż. Andrzej Pierończyk) and to demonstrate the Controller's accountability. The Policy is the overarching document in relation to specific instructions, registers and forms concerning data protection, information security and document management.

The Policy applies to the manufacturing and administrative processes of the plant, in particular in the handling of industrial customers, preparation of quotations, analysis of technical documentation, order execution, quality control, logistics, purchasing, accounting, HR, recruitment, cooperation with suppliers and subcontractors, and the reception of guests.

§ 2. Data Controller

The Controller of personal data is Ślusarstwo Produkcyjne inż. Andrzej Pierończyk, ul. Budowlana 5, 41-100 Siemianowice Śląskie, NIP 6430003808, REGON 270579373, BDO 000245386, e-mail: biuro@pieronczyk.pl. The Controller determines the purposes and means of processing and is responsible for implementing organisational and technical measures appropriate to the risk.

§ 3. Personal scope

The Policy is binding on all persons who process data on behalf of or for the benefit of the Controller, irrespective of the basis of cooperation, including:

- the owner, management and persons authorised to represent the company;
- employees, contractors, B2B collaborators, trainees and interns;
- persons involved in recruitment, HR, accounting, administration, purchasing, sales, logistics, quality, production and maintenance;
- subcontractors, service providers, IT service providers, accountants, legal advisors, HR advisors and other data processors;
- guests, auditors, representatives of customers and suppliers present on the company's premises in connection with its activities.

§ 4. Data Protection Officer

At the time of preparation of this version of the Policy, the document assumes that the Controller does not appoint a Data Protection Officer, unless a separate assessment indicates an obligation or advisability to do so. The assessment of grounds for appointing a DPO should be carried out at least once a year and following a material change in the scale or nature of data processing. At the date of approval of the Policy, the Controller does not meet the criteria for mandatory appointment of a DPO under Art. 37(1) GDPR: the core activities of SPP do not consist of processing operations that require regular and systematic monitoring of data subjects on a large scale, nor of large-scale processing of special categories of data. The Controller documents the decision not to appoint a DPO with a statement of reasons.

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

CHAPTER II. CATEGORIES OF PERSONS, DATA AND PROCESSING OPERATIONS

§ 5. Categories of persons

- job applicants, employees, former employees and family members of employees to the extent required by employment and social insurance law;
- associates, contractors, subcontractors and persons acting on behalf of counterparties;
- representatives of customers, suppliers, business partners, certification bodies, auditors, carriers and technical service providers;
- guests of the plant, persons booking visits, meeting participants and persons submitting technical drawings or requests for quotation;
- persons making contact by e-mail, telephone, the website or traditional correspondence;
- persons recorded by CCTV if present in monitored areas.

§ 6. Categories of data

- identification and contact data: first name, surname, position, company, e-mail address, telephone number, correspondence address;
- HR data: national ID number (PESEL), date of birth, address, employment documents, qualifications, H&S; training records, licences, medical examinations, remuneration, leave, ZUS and tax documentation;
- recruitment data: CV, qualifications, licences, experience and contact details;
- contractual and accounting data: data of counterparty representatives, orders, invoices, contracts and correspondence;
- technical and quality data: data of persons involved in project correspondence, approvals, audits, acceptance tests and complaints;
- IT data: logins, user IDs, system logs, IP addresses, access and change history;
- visitor and plant security data: first name, surname, company, purpose of visit, person visited, entry and exit time, and optionally vehicle registration number and image captured by CCTV.

§ 7. Special categories of data and criminal data

Special categories of data, in particular health data, may be processed only to the extent required by employment, H&S;, occupational medicine, social insurance law or other legally permissible cases. Data relating to criminal convictions and offences are not processed unless a specific legal provision permits or requires their collection.

CHAPTER III. PRINCIPLES OF PERSONAL DATA PROTECTION

§ 8. Core principles

The Controller and authorised persons apply the principles of: lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; and accountability. Each processing operation should have an identified purpose, legal basis, data scope, recipients, retention period and security measures.

§ 9. Legal bases for processing

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

- necessity for the conclusion or performance of a contract, including an employment contract, commercial contract, order or subcontracting agreement;
- legal obligation in the field of employment law, taxation, accounting, H&S;, social insurance and archiving;
- legitimate interest of the Controller, e.g. contact with counterparty representatives, pursuit of claims, plant security, asset protection and correspondence management;
- consent of the data subject where required by law or where data are processed beyond the primary purpose;
- protection of vital interests of a natural person in exceptional situations involving a threat to life or health.

§ 10. Prohibition on unjustified copying of documents

Identity cards, driving licences, passports, ID documents, payment cards, medical records or documents containing special categories of data shall not be copied unless this follows directly from a legal provision or a documented need. If it is sufficient to confirm information, the fact of verification should be noted without reproducing the entire document.

CHAPTER IV. ORGANISATION OF INFORMATION SECURITY

§ 11. Organisational security

- access to data is granted on a need-to-know basis;
- access to systems and resources is personal and may not be shared;
- documents containing personal data are stored in places secured against access by unauthorised persons;
- printouts, notes, technical documentation and data carriers must not be left unattended in publicly accessible locations;
- data transmitted electronically are protected in a manner appropriate to their sensitivity, e.g. by password, encryption, limiting recipients or sending the password separately;
- access of external persons to premises, systems or documentation is permitted only to the necessary extent and under the supervision of the responsible person.

§ 12. Technical and IT security

IT systems, e-mail, network drives, computers, laptops, mobile devices, machines with network interfaces and external media should be secured in accordance with the minimum IT requirements set out in Annex 8. Backups should cover data essential for business continuity, including commercial, HR, accounting, technical and quality documentation. The Controller or a designated person periodically verifies that backups are being made and can be restored.

§ 13. Technical documentation and customer data

Technical drawings, models, requests for quotation, production documentation, quality documents, material certificates, welding documentation and project correspondence may contain personal data of employees of customers, suppliers, designers, auditors or persons approving documentation. Access to documentation is granted exclusively to persons involved in the relevant process. Customer documentation shall not be sent to private e-mail accounts or stored on private devices.

CHAPTER V. AUTHORISATIONS, CONFIDENTIALITY AND TRAINING

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

§ 14. Authorisations and register

Access to personal data may be granted only to a person authorised by the Controller or a person designated by the Controller. The authorisation specifies the person, position or role, scope of data, systems or documentation, purpose of access and the date of granting and withdrawal of rights. The Controller maintains a register of authorised persons.

§ 15. Confidentiality

Every authorised person is obliged to maintain the confidentiality of personal data, technical and commercial information and other information not intended for public disclosure. The obligation of confidentiality continues after the termination of employment or cooperation.

§ 16. Training and awareness

Persons processing data should be familiarised with this Policy before gaining access to data. Training or instruction covers GDPR principles, confidentiality, IT security, incident reporting, clean desk policy, secure correspondence and the rules for transferring technical documentation.

CHAPTER VI. PROCESSING RECORDS, INFORMATION OBLIGATIONS AND DATA SUBJECTS' RIGHTS

§ 17. Record of processing activities

The Controller maintains a Record of Processing Activities in accordance with Annex 1. The Record covers purposes, categories of persons and data, legal bases, recipients, processors, systems, data locations, transfers, deletion periods and a general description of security measures. The Record is updated when a new process, system or supplier is introduced, upon a material change in data scope or following an audit.

§ 18. Information obligations

The Controller provides data subjects with the information required by the GDPR at the time of data collection or within another period prescribed by law. Information clauses are set out in Annex 10 and should be adapted to the actual process, recipients, retention periods and systems used.

§ 19. Rights of data subjects and handling of requests

Data subjects have the rights provided for in the GDPR, including the right of access, rectification, erasure, restriction of processing, data portability, objection, withdrawal of consent and the right to lodge a complaint with a supervisory authority. Requests from data subjects are accepted by the owner, the person coordinating data protection or the person designated to handle the relevant process. The procedure and request register are set out in Annex 4.

CHAPTER VII. RETENTION, ARCHIVING, PROCESSORS AND TRANSFERS

§ 20. Data retention

Personal data are retained for the period resulting from the purpose of processing, legal provisions, the duration of the contract, the limitation period for claims or a justified evidentiary need. Upon expiry of the retention period, data shall be deleted, anonymised or transferred to the archive in accordance with security principles. The detailed retention schedule is set out in Annex 3.

§ 21. Processors and data disclosure

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

Before allowing an external entity access to data, the Controller assesses whether the entity acts as a processor, independent controller, joint controller or data recipient. If the entity processes data on behalf of the Controller, a data processing agreement must be concluded or an equivalent legal basis ensured. The list of processors and recipients is set out in Annex 2.

§ 22. Transfers outside the EEA

Personal data are not transferred outside the European Economic Area without prior verification of the legal basis for the transfer, safeguards and documentation required by the GDPR. This applies in particular to cloud services, e-mail tools, file-sharing systems, remote IT support and subcontractors located outside the EEA.

CHAPTER VIII. BREACHES, RISK ASSESSMENT, DPIA AND PRIVACY BY DESIGN

§ 23. Incident and breach reporting

Every person who notices or suspects a personal data breach is obliged to report the incident immediately to the owner, their supervisor or the person coordinating data protection matters. The report is to be made regardless of whether the breach was caused by the reporting person. The form, register and decision matrix are set out in Annex 5.

§ 24. Assessment and notification of a breach

After receiving a report, the Controller establishes the facts, scope of data, number of persons affected, possible consequences, cause of the incident and remedial measures. Every breach is documented, even if it does not require notification to the supervisory authority. If the breach is likely to result in a risk to the rights and freedoms of natural persons, the Controller notifies the supervisory authority without undue delay, and in principle no later than 72 hours after becoming aware of the breach. A delay beyond 72 hours requires a written statement of reasons.

§ 25. Risk assessment and DPIA

The Controller applies a risk-based approach. A risk assessment should be conducted for new systems, processes, significant organisational changes, the introduction of CCTV, cloud services, outsourcing, remote access, processing of special categories of data or breach events. If a planned process is likely to result in a high risk, the Controller carries out a DPIA before commencing processing. The checklist is set out in Annex 9.

§ 26. Privacy by design and privacy by default

When designing new processes, forms, contracts, IT solutions and work organisation, the Controller takes data protection into account from the outset of the project. Default settings should limit the scope of data collected, access, retention period and number of recipients to the minimum necessary for the purpose.

CHAPTER IX. CCTV MONITORING, ACCESS CONTROL AND VISITOR DATA

§ 27. Plant visitors

The entry of external persons onto the plant premises may involve the processing of data necessary for security, visit organisation, trade secret protection, H&S;, audit management or meeting purposes. The scope of visitor data should be limited to the minimum necessary.

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

§ 28. CCTV monitoring

CCTV monitoring is used in accordance with a separate document: SPP CCTV Monitoring Policy. A general information clause and signage for monitored areas are made publicly available. The detailed list of cameras, their locations, observation angles and technical functions is an internal document; it is not published on the website and is available exclusively to authorised persons, system maintenance staff, auditors or authorities with powers under applicable law. SPP does not monitor work e-mail, computer workstation activity or vehicle location (GPS). The introduction of any such form of monitoring would require a prior legal basis, updated documentation and notification of employees in accordance with Article 22(3) of the Labour Code.

CHAPTER X. REVIEWS AND FINAL PROVISIONS

§ 29. Audits and reviews

The Controller reviews this Policy at least once every 12 months, and also following a significant organisational change, introduction of a new system, change in legislation, confirmed breach, customer audit, change of processors or change in the scope of data processed within the company. At the date of approval of the Policy, the number of persons working for the Controller does not reach the threshold of 50, and therefore there is no obligation to implement an internal whistleblowing procedure or to establish a Company Social Benefits Fund; SPP does not maintain such a fund. This status is subject to review if the number of employees increases.

§ 30. Implementation package

The data protection implementation package includes at least: this Policy, the record of processing activities, the list of processors, authorisations, the register of authorised persons, confidentiality declarations, the breach register, the data subject request register, information clauses, the CCTV monitoring policy, the website privacy policy, the IT access granting and revoking procedure, and employee acknowledgements of receipt of the Policy.

§ 31. Final provisions

The Policy enters into force on the date of its approval by the Controller. Any derogation from the Policy requires the consent of the Controller or a person designated by the Controller and should be documented if it may affect the rights or freedoms of natural persons. This document is an internal document of the Controller.

Prepared / verified

.....
date and signature

Approved — Controller / Employer

.....
date and signature