Privacy Policy

pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the instruction of data subjects (hereinafter the "GDPR") and pursuant to Act No. 110/2019 Coll., on personal data processing

Thank you for visiting our website.

I. WHO WE ARE:

The business company **Zelinger plast s.r.o.**, with its registered office at Tečovice 421, 763 02 Zlín 4, business ID number: 60750774, tax ID number: CZ60750774, registered in the Commercial Register kept by the Regional Court in Brno, file C 19212 (hereinafter "Zelinger plast" or the "Controller").

Our company operates in the field of plastic production and provides services exclusively to business entities. We process data subjects' personal data when carrying out our business activities.

In connection with our activities, contractual relationships and also when visiting our website, some personal data are processed. In order to provide you with a clear and understandable overview of how we handle these data, we have prepared this Privacy Policy (hereinafter the "Policy").

The security and protection of your personal data are of key importance to us. We therefore want to tell you what information we collect and for what purposes we use it.

The aim of this Policy is to inform suppliers, customers, business partners and visitors of their rights in accordance with GDPR.

Terms used:

PD	personal data, i.e. all information leading to the identification of a specific natural person
PD Subject	A subject whose personal data Zelinger plast processes
Controller	Zelinger plast, the company that records, processes, archives and protects your personal data

II. CONTACT DETAILS FOR THE CONTROLLER

Who to contact if you have any questions or requests for information regarding PD:

Zelinger plast s.r.o., with its registered office at Tečovice 421, 763 02 Zlín 4
Controller's contact person in GDPR matters: Marie Bazalková
Phone number: 778 441 216
E-mail address: marie.bazalkova@zelinger.cz

III. MAIN OBJECTIVES OF PERSONAL DATA PROTECTION

- Ensuring the protection of natural persons' rights with regard to the processing of their PD.
- Maintaining continuous compliance with the GDPR's requirements.
- Maintaining compliance with other legal and technical requirements laid down in related legal regulations and standards.
- Ensuring the ability to prevent and manage adverse events relating to GDPR.
- Continuous improvement of the suitability, adequacy and effectiveness of the PD protection management system

IV. CATEGORIES OF PD THAT ARE SUBJECT TO PROCESSING

With regard to personal data protection, we limit the processing of personal data to data that are reasonable and relevant for the appropriate contractual or business purpose. We process only personal data necessary for your identification, communication with each other and to fulfil our contractual and business obligations, always to the extent specified by the relevant legal regulations.

Categories of personal data we process:

1. **Identifying information** used to uniquely and unmistakably identify a PD Subject (i.e. corporate name, first name, last name, title, business ID number, tax ID number);
2. **Contact details** (e-mail address, phone number, registered office);
3. **Financial or banking information** (billing information – bank account number, bank);
5. Data necessary for the fulfillment of a contract or processed based on a legal obligation (data about orders, etc.);
6. **Data provided voluntarily** (If you provide us with any other data voluntarily (e.g. photos for publication on the website or in PR materials), we process them only with the consent of the person concerned;
7. **Audiovisual data** (image recorded by a CCTV system with recording);
8. **Web technical logs** (As part of your visit to our website, the following technical data necessary for the secure operation of the website may be processed: IP address, date and time of access to the website, information about your internet browser, operating system, online behavior data);
9. **Employees** Our employees' personal data are not described in detail in this Policy. The processing of employment law and personal data is governed by a separate internal Employee Data Protection Directive, which is not intended for the public. This directive sets out the purposes, scope of processing, retention period and security measures in accordance with the GDPR and relevant employment legal regulations.

V. SCOPE OF PROCESSING OF PD

We process personal data only to the extent necessary for communication, fulfillment of contractual obligations, bookkeeping, security of operations and property protection. In particular, we obtain data directly from data subjects as part of mutual communication, during conclusion or fulfillment of a contract, or from publicly available sources (e.g. the Commercial Register, ARES). We only process personal data where required to do so by applicable legal regulations or where necessary to protect our legitimate interests.

We do not request consent to the processing of personal data, except in situations where the processing is based on voluntary provision of data for a specific purpose (e.g. publication of photographs).

VI. SOURCES OF PD

We obtain PD:

a. directly from the PD Subject (in the course of normal business communication between companies, in particular via e-mail, telephone or a personal meeting. We also obtain data when preparing or fulfilling contractual relationships between firms);

b. from business partners or suppliers (we process the contact details of persons acting on behalf of our suppliers, purchasers or contractual partners, if such persons are designated as contact persons or persons authorized to negotiate or fulfill a contract);

c. from publicly available sources (we use information from public registers and databases (e.g. the Commercial Register, ARES) or from publicly available company websites, solely for the purpose of establishing or fulfilling a business relationship);

d. from third parties who are authorized to provide the data (in some cases, personal data may be provided by a person authorized to do so – for example, an authorized employee of a business partner or a carrier);

e. from the CCTV system at the Controller's registered office. Images are recorded in the company's premises in order to protect persons and property. Detailed information about the processing of personal data by the CCTV system is provided in the *internal Directive on Protection and Processing of Personal Data – CCTV System S-1-007,* which is available on request at the company's registered office.

VII. PURPOSES OF PROCESSING PD

In accordance with Article 6.(1) GDPR, the Controller may process data without the PD Subject's consent only to the extent necessary for the given purpose and for the period necessary to achieve the purpose, provided that:

- processing is necessary for the fulfillment of a contract to which the PD Subject is a party or for the performance of measures taken prior to the conclusion of a contract at the PD Subject's request;
- processing is necessary to fulfil legal obligations to which the Controller is subject (e.g. the Archiving Act);
- processing is necessary for the purposes of the Controller's legitimate interests, except where the interests or fundamental rights and freedoms of the PD Subject requiring the protection of personal data prevail over these interests (e.g. ensuring the security and protection of property (CCTV system), protection of rights and assertion of legal claims, management and optimization of internal processes, recording of business negotiations, ensuring the functionality and security of the website).
- processing for the purposes contained in the consent to personal data processing granted by the PD Subject under the terms of the GDPR. We only use consent in specific situations where the processing is voluntary and not related to the fulfillment of a contract – e.g. photographs for the company's presentation. If we process your personal data based on consent, you can rescind it at any time using the contact details provided in this Policy. The rescinding of consent does not affect the lawfulness of the processing carried out before its rescinding.

VIII. CATEGORIES OF PD SUBJECTS

We process personal data only for the following categories of data subjects:

Representatives of suppliers, purchasers and contractual partners
(company contact persons, persons acting on behalf of legal entities, self-employed persons).
Natural persons entering the company premises
(e.g. carrier drivers, visitors, service technicians).
Persons captured by the CCTV system
(visitors, suppliers, drivers, other natural persons present in the monitored area).

Notifiers of unlawful conduct
(natural persons using the internal notification system pursuant to Act No. 171/2023 Coll.).

Personal data of employees and job applicants are processed separately within the framework of an internal directive and are not subject to this public policy.

IX. CATEGORIES OF RECIPIENTS OF PD - who will receive my data?

We share your personal data only to the extent necessary and only if there is a legal reason for doing so, in particular a legal obligation, fulfillment of a contract or a legitimate interest of the Controller. **Recipients are always required to ensure an adequate level of protection of personal data.**

1) **Public authorities**
   e.g. government authorities, courts, the Police of the Czech Republic, tax office, health insurance companies and the Czech Social Security Administration, if required by legal regulations.
2) **External processors of personal data**

- external accounting office;
- external IT company;
- suppliers of production systems;
- transport and forwarding companies;
- hosting service or web service providers.

These processors act on the basis of contracts pursuant to Art. 28 GDPR and are bound by confidentiality.

3) **Contractual partners** in cases where it is necessary to fulfill a contract (e.g. material suppliers, purchasers, service technicians).
4) **Third parties based on explicit consent**
   only in specific and exceptional situations, e.g. when posting photographs on the website or in promotional materials.

X. METHOD OF PROCESSING AND PROTECTION OF PD

Personal data processing is carried out by the Controller or by the processors authorized by it with whom the Controller has concluded a contract pursuant to Art. 28 GDPR. These contracts guarantee that the processors comply with all data protection obligations and respect data subjects' rights.

The processing takes place at the Controller's registered office. Personal data are processed using computer technology or manually in paper form, always in accordance with security principles and with regard to minimizing risks.

The Controller has taken and maintains technical and organizational measures to protect personal data, in particular measures against unauthorized or accidental access, alteration, destruction, loss, unauthorized transfer or other misuse of personal data. These measures include, but are not limited to, checking access rights, securing IT infrastructure, regular system updates and employee training.

Personal data are accessible only to persons who strictly need them to perform their work or fulfill contractual obligations. Employees of the Controller who have access to personal data are bound by a confidentiality obligation. The same rules also apply to employees of processors who process personal data to the extent necessary to provide services to the Controller.

XI. HOW IS MY DATA PROCESSED IN THE FOLLOWING PROCESSING OPERATIONS:

There is no automated decision-making in individual cases, including profiling. Conclusion and fulfillment of a contract

In connection with the conclusion of contracts, we only process personal data that are necessary to conclude or fulfill a contractual relationship between companies. Typically, this includes: first and last name of the contact person, job title, business name or business ID number (with the self-employed), contact details (phone number, e-mail address). Other data may only be processed if they are necessary for the implementation of specific business cooperation.

We store personal data processed in connection with a contractual relationship for the duration of the contract and subsequently for 4 years after its termination to protect legal claims.

Visiting our website

When you visit our website, technical data that your browser transmits to the server are automatically collected. These are, in particular:
your IP address, the date and time of access, the URL visited, the browser and operating system type, the URL of the page from which you came to the website.

These data are processed based on the Controller's legitimate interest – ensuring the security of the website and its proper functioning. The provision of these data is technically necessary to display the website.

We retain technical logs only for as long as necessary, typically for a maximum of 30 days, unless a legal regulation or security incident requires longer retention.

Contact form

There is a contact form on our website that you can use to contact us with questions, inquiries or other suggestions.

When submitting the form, we process the following data: first and last name, e-mail address, text of the message, information about granting consent to the processing of personal data.

Data processing is based on the consent pursuant to Art. 6(1)(a) GDPR that you give before submitting the form (checkbox) or on the fulfillment of a contract / negotiation prior to conclusion of a contract pursuant to Art. 6(1)(b) GDPR, if your message relates to a business relationship, offer or inquiry.

The purpose of processing is to respond to your message, answer your inquiry or contact you in response to your question.

We only store the data submitted via the contact form for as long as necessary. If the form is submitted based on consent pursuant to Art. 6(1)(a) GDPR, we will retain the data for three (3) years after the processing of your request or until the rescinding of consent, but no later than 30 days after its rescinding

If your message relates to an existing or future contractual relationship, the data are processed based on Art. 6(1)(b) GDPR and stored for the duration of the business relationship and subsequently for three (3) years to protect legal claims and prove communication within the limitation periods.

Visit to the Controller's registered office

The CCTV system is operated on the company's premises in order to protect property, ensure the safety of persons and prevent harmful events. The legal basis for processing is the Controller's legitimate interest pursuant to Art. 6(1)(f) GDPR.

Before the CCTV system was put into operation, the Controller conducted a balancing test to assess the degree of interference with natural persons' rights and freedoms and took measures to minimize interference with their privacy.

The CCTV system records images of persons moving around the monitored areas. The records are stored for a maximum of 14 days, after which they are automatically and irreversibly deleted, unless longer retention is necessary to deal with a security incident or based on the legitimate requirements of law enforcement authorities.

Detailed information on the processing of personal data through the CCTV system is provided in the *Directive on Protection and Processing of Personal Data – CCTV System S-1-007,* available on request at the company's registered office.

Upon entering the Controller's premises, the statement of basic data for the visitor sign-in sheet may be required. The data processed includes: the visitor's first and last name, the company name (in case of a business visit), the person or department the visitor is coming to see, the time of arrival and the time of departure.

The purpose of processing is the protection of Controller's property, ensuring the safety of persons and control of the movement of persons on the premises. The legal basis is the Controller's legitimate interest pursuant to Art. 6(1)(f) GDPR.

Sign-in sheets are kept for 14 days, after which they are securely shredded. Personal data are not passed on to third parties, except in situations where this is necessary to deal with a security incident, insurance event or based on a legal requirement by public authorities.

XII. DURATION OF PROCESSING OF PD

The Controller keeps the PD only for the period necessary to fulfil the purpose. For which they were collected or for the period prescribed by legal regulations.

The retention period varies according to the type of processing.

For example, we store personal data contained in accounting and tax documents (e.g. invoices) for at least 10 years in accordance with the Accounting Act and the VAT Act. Personal data processed based on consent (e.g. photographs, voluntarily provided materials) are stored for a maximum of 3 years from the end of the last business relationship or until the rescinding of consent.

After rescinding, we will erase them within 30 days at the latest. We keep personal data relating to a report for 5 years in accordance with Act No. 171/2023 Coll.

Erasure after the end of the purpose

After the relevant retention period, personal data are:

- erased;
- anonymized; or
- securely destroyed;

  if there is no legal reason for their continued retention.

Detailed information on specific retention periods is available upon request.

XIII. TRANSFER OF DATA OUTSIDE THE EU

Where we use the services of various external suppliers (e.g. software tools, cloud solutions, hosting), personal data may be transferred outside the EU, in particular to the USA (Microsoft, Google, Meta, cloud services), if necessary.

We always carry out such transfers in full compliance with Chapter V of Regulation (EU) 2016/679 (GDPR), i.e. either based on a decision by the European Commission on ensuring an adequate level of protection of personal data, through standard contractual clauses ("Model Clauses") approved by the European Commission or by using another legally permissible mechanism for data transfer outside the EEA.

XIV. TECHNICAL AND ORGANIZATIONAL SECURITY

We have implemented and maintain appropriate technical and organizational measures, internal control processes and information security appropriate to the risks associated with personal data processing.

These measures aim to ensure the confidentiality, integrity and availability of personal data and to minimize the risks of misuse, loss or unauthorized access.

The measures include, in particular:

- restricting access to personal data to authorized employees only, always to the extent necessary for the performance of their work duties;
- regular training of employees on personal data protection and information security;
- control of access permissions in individual systems according to functional roles (business, economic and manufacturing departments have access only to data necessary for their activities);
- ensuring secure infrastructure, including server administration, data backup and protection against cyber threats;
- physical security of the premises where personal data are stored or processed;
- confidentiality obligations for all employees and processors who have access to data.

The Controller does not collect any data falling into special categories of personal data pursuant to Art. 9 GDPR.

If the Controller concludes a contract with an external supplier as a part of which the processing of personal data is to be carried out by a third party, a written contract on personal data processing containing all the elements required by the GDPR and ensuring an appropriate level of security is concluded with the processor.

XV. RIGHTS OF PD SUBJECT

At any time during the processing of PD, the PD Subject may exercise the following rights in accordance with Art. 12 GDPR:

- **Right to Information**: you can request information about what personal data we process about you;
- **Right to rectification:** if the data are inaccurate or incomplete;
- **Right to erasure**: if processing is not necessary, you can request the erasure of the data;
- **Right to restrict processing:** you can request restricted use of data, e.g. if you contest their accuracy or legality;
- **Right to data portability**: if you have provided us with personal data within the scope of consent pursuant to Art. 6(1) GDPR or under a contract pursuant to Art. 6(1)(b) GDPR, you can request that they be transferred to another Controller;
- **Right to object:** to the processing of your personal data carried out based on a legitimate interest;
- **Right to rescind consent:** where processing is based on consent, you can rescind it at any time, with effect for the future;
- **Right to lodge a complaint** with a supervisory authority pursuant to Art. 77 GDPR if you believe that the processing of your personal data violates the GDPR. The supervisory authority is: **Office for Personal Data Protection, address: Pplk. Sochora 27, 170 00 Prague 7, tel.: +420 234 665 111; for consultations regarding GDPR, use the specially created hotline +420 234 665 800 and e-mail address: posta@uoou.cz.** More information is available on the website of the Office for Personal Data Protection – https://uoou.gov.cz/kontakt.

If you wish to exercise any of your rights set out in this Policy or have a question regarding the processing of your personal data, you **may contact us using the contact details stated in this Policy above.**

We will respond to your requests without undue delay, within no more than 30 days in accordance with Art. 12 GDPR. In justified cases, the period may be extended by another two months, which we will inform you of.

XVI. PROCESSING OF PERSONAL DATA ABOUT EMPLOYEES

Information on the processing of personal data of employees and personal data of persons working with the Controller is provided in a separate internal document available on the Controller's intranet.

XVII. COOKIES

Our website uses cookies. Detailed information on the types of cookies, the purposes and options for setting them can be found in the separate "Cookies" section of our website. Cookie settings can be easily changed by a user of the Zelinger website at any time by clicking on the link provided.

XVIII. UPDATING THE POLICY

We review and update this document regularly and reserve the right to amend it. Any changes to this Policy are effective from the date the updated version of the Policy is posted on the company's website.

This Policy was last updated on 30 October 2025.

Ing. Lenka Horáková,
CEO of Zelinger plast s.r.o. (CEO)

www.zelinger.cz | mobile phone: +420 777 714 721 | zelinger@zelinger.cz | Tečovice 421 | 763 02 Tečovice | EN