

Progrits Group Privacy Policy

Contents

1	Background and purpose.....	2
2	Policy statement.....	2
2.1	Personal Data We Process	2
2.2	Purpose and Legal Basis for Processing	3
2.3	Data Processing Principles	3
2.4	Data Subject Rights	3
2.5	Data Sharing and Transfers	4
2.6	Data Security.....	4
2.7	Retention Policy.....	4
2.8	Complaints and Supervisory Authority	4
3	Target audience	4
3.1	Progrits Group.....	4
3.2	Employees.....	5
4	Roles and responsibilities	5
5	Exceptions.....	5
6	Monitoring of compliance	5
7	References.....	5

1 Background and purpose

Progrits mission is to acquire, advance and expand niched software companies by bringing hands-on experience, synergistic business infrastructure, technical platforms as well as capital for future development. We do this pragmatically by knowing our customers' business and by being dedicated professionals with grit.

To ensure that the Progrits Group (see definition of the Group in section 3.1) complies with applicable laws and regulations and that the Group's values and ways of working are valid throughout the entire organisation, the Group has developed a number of group-wide policies, including this Policy.

2 Policy statement

At the Progrits Group, we prioritize the privacy and security of our customers, partners, and employees. As a group of software companies delivering cloud and on-site Software-as-a-Service (SaaS) solutions to primarily business-to-business (B2B) customers, we are committed to protecting personal data in compliance with the General Data Protection Regulation (GDPR), Regulation (EU) 2016/679, and other applicable data protection laws.

This Privacy Policy outlines how we collect, use, store, and protect personal data, ensuring transparency and accountability in all our operations. The policy is subject to regular updates and has been approved by the Board of Directors. It is effective immediately upon its publication on our public website.

This policy covers all processing of personal data, including:

- Personal data of employees, clients, vendors, and other business partners.
- Data collected during the delivery of cloud and on-site SaaS services.
- All personal data processed by the Group, whether processed in digital or physical format.

2.1 Personal Data We Process

We collect and process the following types of personal data:

- **Customer Data:** Information related to our B2B customers, including contact details of company representatives (e.g., name, email, phone number), contract details, and billing information.
- **Employee Data:** Information related to our employees, such as name, address, contact information, identification number, payroll details, and any other relevant HR data.
- **Supplier and Partner Data:** Information related to the contact persons of our suppliers and partners.
- **Usage Data:** Data collected through our SaaS services, including IP addresses, user activity logs, and other operational data necessary to deliver, improve, and secure our services.

We do not process any sensitive personal data unless explicitly necessary, and we ensure that all such processing adheres strictly to GDPR requirements.

2.2 Purpose and Legal Basis for Processing

We process personal data only when there is a legal basis to do so, which includes:

- **Performance of Contract:** Personal data necessary for fulfilling contractual obligations with our customers, business partners and employees.
- **Legal Obligations:** Compliance with legal requirements, such as accounting, tax laws, and regulatory reporting.
- **Legitimate Interest:** Processing based on the legitimate interests of the Group, such as improving our services, maintaining security, and building business relationships, balanced against the individual's rights.
- **Consent:** Where required, we obtain explicit consent from the data subject for specific types of data processing.

2.3 Data Processing Principles

In all our activities, we adhere to the following core principles for processing personal data:

- **Lawfulness, Fairness, and Transparency:** We process personal data in a lawful, fair, and transparent manner.
- **Purpose Limitation:** Personal data is collected for specified, explicit, and legitimate purposes and is not processed further in a manner incompatible with those purposes.
- **Data Minimization:** We collect only the personal data necessary for the purposes for which it is processed.
- **Accuracy:** We ensure that personal data is accurate and, where necessary, kept up to date.
- **Storage Limitation:** Personal data is not stored for longer than necessary for the purposes for which it is processed.
- **Integrity and Confidentiality:** Personal data is processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing, accidental loss, destruction, or damage.

2.4 Data Subject Rights

Under the GDPR, individuals whose personal data we process have the following rights:

- **Right of Access:** Request access to their personal data and information about how we process it.
- **Right to Rectification:** Request the correction of inaccurate or incomplete personal data.
- **Right to Erasure ("Right to be Forgotten"):** Request deletion of personal data, subject to legal obligations or legitimate interests.
- **Right to Restriction of Processing:** Request restriction of processing under certain circumstances.
- **Right to Data Portability:** Receive a copy of their personal data in a structured, commonly used, and machine-readable format, and request its transfer to another data controller.
- **Right to Object:** Object to the processing of personal data based on legitimate interests, direct marketing, or profiling.
- **Right to Withdraw Consent:** If the processing is based on consent, the individual can withdraw their consent at any time.

To exercise any of these rights, individuals can use the contact details under section 4.

2.5 Data Sharing and Transfers

We may share personal data with third parties in the following cases:

- **Service Providers:** We may share personal data with trusted third-party service providers who assist us in delivering our services, such as cloud service providers, data storage solutions, and IT support.
- **Legal and Regulatory Authorities:** Where required by law or for compliance with regulations, we may share personal data with governmental authorities or regulators.
- **Group Companies:** Personal data may be shared within the Group for operational purposes.

When transferring personal data outside the European Economic Area (EEA), we ensure adequate safeguards are in place, such as the use of Standard Contractual Clauses (SCCs) or ensuring the recipient country has adequate data protection laws.

2.6 Data Security

We implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk of processing personal data. This includes:

- Encryption of sensitive data.
- Regular audits and assessments of security practices.
- Restricting access to personal data to authorized personnel only.
- Regular staff training on data protection and privacy matters.

In the event of a data breach, we have established protocols to assess, manage, and report the breach to relevant authorities and affected individuals as required under GDPR.

2.7 Retention Policy

We retain personal data for as long as necessary to fulfil the purposes for which it was collected, or to comply with legal, regulatory, or contractual obligations. Once the data is no longer needed, we securely delete or anonymize it.

2.8 Complaints and Supervisory Authority

If you believe we have breached your privacy rights or have concerns about how we process personal data, you can lodge a complaint with the Group CEO (see section 4 for details). Additionally, you have the right to contact the relevant supervisory authority, which in Sweden is the Swedish Authority for Privacy Protection (IMY) – see section 7 for details.

3 Target audience

3.1 Progrits Group

For this Policy, Progrits Group means any entity over which Progrits AB has control (or joint control). Progrits AB controls an entity when Progrits AB directly or indirectly:

- i. owns more than half the share capital of the entity, or
- ii. owns more than half the voting rights of the entity, or
- iii. has the power to appoint more than half of the board of directors of the entity or similar governing body legally representing the entity, or
- iv. has the right to manage the entity's affairs.

3.2 Employees

This policy applies to all employees and is also directed to all external interested parties.

4 Roles and responsibilities

The Group CEO is the owner of this Policy. The Board of Directors is authorized approver of this Policy. The respective Group subsidiary business units operate as the data controller for all personal data processed by and in the software services they provide to customers. The Group operates as the data controller for all personal data processed by the Group functions and the Group parent company Progrits AB. For any questions regarding this policy or how we process personal data, please contact:

Group CEO Björn Ekström

Privacy@progrits.se

Västra Hamngatan 5, 411 17 Göteborg

5 Exceptions

No exceptions are allowed to this Policy, unless otherwise approved by the Board of Directors.

6 Monitoring of compliance

Compliance with this policy shall be monitored continuously. Objectives and goals are to be set as part of Information security objectives by the Group business units and are evaluated annually during the Management review.

7 References

EU Standard Contractual Clauses (SCCs): https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en

Contact Details of IMY:

Website: <https://www.imy.se/en/>

Phone: +46 8 657 6100

Email: imy@imy.se