PRIVACY AND DATA PROTECTION POLICY FOR SUPPLIERS

A STIHL Ferramentas Motorizadas Ltda. ("STIHL") is committed to respect the privacy and protection of personal data of all its stakeholders, including its Suppliers. STIHL seeks Suppliers who share this commitment when processing personal data on behalf of STIHL or under its contracts. This Privacy and Data Protection Policy for Suppliers ("Policy") informs about STIHL's Personal Data protection practices and about Suppliers' obligations regarding the Processing of Personal Data, within the scope of the business relationship. Any future contract mutually accepted and entered into between the Supplier and STIHL may complement or change this Policy. In case of contradiction or conflict between this Policy and the contract, the provisions of such contract shall prevail.

For the purposes of this Policy, all terms initiated in capital letters and not specifically defined in this instrument shall have the meaning attributed to them by LGPD (Law No. 13.709/2018).

HOW WE HANDLE PERSONAL DATA OF SUPPLIER REPRESENTATIVES

The Supplier acknowledges that, in the course of its business relationship, STIHL may periodically treat Personal Data related to employees or individuals who act on behalf of the Supplier in the provision of services ("Representatives"). It is the responsibility of the Supplier, acting as Controller of the Representatives' Data, to ensure that **(a)** the Data received by STIHL is collected and shared in accordance with applicable legislation and **(b)** the Representatives are informed about the Personal Data treatment activities performed by STIHL, as described in this Policy.

What Personal Data do we treat and what is the purpose of the treatment?

STIHL collects and stores Personal Data minimally necessary for the management of the business relationship with the Supplier, especially identifying Personal Data, such as name, social security numbers, date and place of birth, marital status, telephone, e-mail and home address, position, t-shirt size, labor registration number and/or *FRE* and *ASO*. Among the main purposes for the treatment of Personal Data are:

- ✓ Registration of Suppliers;
- ✓ Obtaining quotations and price quotes for contracting services or making purchases;
- ✓ Purchase air or ground tickets and lodging;
- ✓ Register for discounts on the purchase of STIHL products;
- ✓ Register participants in events organized by STIHL, produce T-shirts, badges and release of entry;
- ✓ Execution of contracts, draft of powers of attorneys and issuance of purchase orders;
- ✓ Management of Suppliers and Representatives, including registration in systems and platforms used (Online Supplier, Pool4Tool, *Colaboration*, etc. or others that may replace them);
- ✓ Receive products or services, allowing and controlling access to STIHL ' s systems and facilities;
- ✓ Billing and accounting management;
- ✓ Financial Evaluation and Due Diligence of Suppliers;
- ✓ Support of business relationship with the Supplier;
- ✓ Confirm the connection between the Representative and the Supplier
- ✓ Compliance with legal and regulatory requirements;
- ✓ Evaluation of legal documents relating to employees of suppliers who provide services for STIHL;

How do we collect or receive Personal Data?

As part of the process of budgeting, formalization and performance of contracts with Suppliers, STIHL will collect or receive Personal Data from Supplier Representatives through contracts, forms, devices, interactions with purchasing teams, e-mails, access to our systems and websites, among others. We may also receive Personal Data directly from the Representative (for example, when registering, contacting us, or accessing our systems and platforms made available by STIHL).

What are the legal bases for the treatment of Personal Data?

The hypotheses for the treatment of Personal Data are listed in Article 7 of the LGPD. Regarding the treatment of Personal Data indicated in this Policy, the legal basis used by STIHL are: (i) contract execution and performance; (ii) fraud prevention; (iii) compliance with legal obligations; (iv) regular exercise of rights and (v) legitimate interest.

Who will be able to access the Personal Data?

Personal Data will only be accessible, at the limit and as needed, by a limited list of recipients within STIHL or STIHL group companies. Personal Data may also be shared with service providers acting on behalf of STIHL (e.g., IT service providers, travel agencies and providers of ordinance and security services) and with government agencies (e.g., tax authorities). Whenever Personal Data are shared with third parties, STIHL will take appropriate measures to ensure that the treatment occurs with the same level of protection provided by this Policy.

How do we store Personal Data?

Personal Data are stored on servers located at STIHL. When storing Personal Data, we implement technical, administrative and contractual security measures to protect them from unauthorized access, disclosure, use, modification, loss or destruction.

When Personal Data are transferred outside of Brazil, STIHL uses appropriate security measures so that the transfer is carried out in accordance with this Policy and as permitted by applicable data protection laws, such as the analysis of the privacy and security standards of third parties, the execution of appropriate contracts and/or internal policies of the STIHL group.

How long do we keep the Personal Data?

We keep Personal Data for as long as necessary to fulfill the purpose for which the Personal Data were collected or until such time as the Personal Data become unnecessary or not pertinent to the intended purposes, except for the provisions in Law, especially considering the following criteria:

- Duration of the contractual relationship;
- Business relationship management;
- Legal and regulatory requirements.

What are the rights of the Holders of Personal Data?

Data Holders have the following rights regarding the treatment of their Personal Data by STIHL:

- The right to confirm that STIHL treats your Personal Data and receive information about the Treatment (including shared use information of Personal Data);
- The right to access, correct and update Personal Data and, in some cases, to oppose the Treatment by STIHL in case of non-compliance with the provisions of LGPD;
- The right to request that your Personal Data be deleted, anonymized or blocked, when unnecessary or excessive, or in case of non-compliance with the provisions of LGPD;
- The right to revoke the consent given for the Processing of Personal Data (when consent is the legal basis used for the Processing);
- The right to file a complaint with the ANPD if it considers that its data protection rights have been violated.

How to Contact Us?

For clarification of doubts regarding this Policy or for the exercise of the rights of the Data Subjects, as established above, it is possible to contact us through our Privacy Portal located at https://www.stihl.com.br/protecao-de-dados-pessoais.aspx or with our Data Protection Officer at the e-mail address privacidade@stihl.com.br.

OBLIGATIONS OF SUPPLIERS IN PROCESSING PERSONAL DATA ON BEHALF OF STIHL OR IN THE CONTEXT OF THE BUSINESS RELATIONSHIP

STIHL expects its Suppliers and other Business Partners, when handling Personal Data on behalf of STIHL or in the scope of the business relationship, to comply with Personal Data protection rules and policies, including LGPD and any other applicable laws and regulations related to the treatment of personal data and privacy, as well as with all guidelines and codes of conduct issued by the Brazilian Data Protection Authority ("ANPD") or other competent authority. This includes, but is not limited to:

1. That Personal Data are treated in accordance with the applicable legislation, including the Processing in accordance with the principles of purpose, adequacy, necessity, free access, quality of data, transparency, security, non-decriminalization, accountability and accountability;
2. Only Treat Personal Data by means of documented instructions from STIHL, and inform immediately if you consider that any instruction from STIHL violates LGPD or any applicable law or regulation;
3. Do not reuse or share Personal Data, unless previously instructed or authorized by STIHL, or if required by applicable law, in which case the Supplier shall inform STIHL about this legal requirement before treatment;
4. Do not transfer Personal Data outside Brazil without prior written approval from STIHL, except when the data transfer occurs to a country recognized by ANPD as having an adequate level of protection;
5. Maintain an internal structure with appropriate technical and organizational measures to ensure that the treatment performed on behalf of STIHL meets the security and confidentiality requirements of LGPD, including the

implementation of appropriate procedures for managing access rights, retention and security of Personal Data;

6. Not to outsource the processing of Personal Data without prior express authorization from STIHL and, even so, always by means of a written contract imposing the same obligations established by STIHL for its Suppliers, including security and confidentiality obligations;
7. Immediately notify STIHL in cases of (i) identification or suspicion of any incident related to the Data (events of unauthorized access or disclosure of Personal Data and/or accidental or unlawful situations of destruction, loss, alteration, communication or any form of improper or unlawful treatment of Personal Data); (ii) any claim or demand related to the treatment of Personal Data, including allegations that the treatment violates the rights of a Data Subject; or (iii) any order, issued by a judicial or administrative authority, requesting the disclosure, access or blocking of Personal Data;
8. Make available to STIHL all information necessary to demonstrate compliance with the obligations listed herein and (i) allow and contribute to audits, including inspections and investigations, and (ii) assist STIHL, including in conducting data protection impact assessments and ensuring the exercise of the rights of the Data Subjects;
9. Take responsibility for the Personal Data Treatment that it performs, obliging itself to keep STIHL free from any obligation and responsibility for any omissions or errors committed by the Supplier - or by any of its employees, agents, representatives, third parties and subcontractors - in the Treatment of Personal Data, if treated in disagreement with the Applicable Legislation or with STIHL's instructions;
10. Delete or return all Personal Data as requested by STIHL after the termination of the services related to the contract and delete existing copies, unless Brazilian law requires the storage of that specific Personal Data;
11. Maintain the confidentiality of all STIHL information you may have access to, protecting it and not disclosing it to third parties, unless the disclosure is previously and expressly authorized by STIHL.

INFORMATION SECURITY PRACTICES

STIHL commits its best efforts to promote a high level of security in the Treatment and storage of Personal Data and confidential information, and expects the Supplier to commit in the same way. Among the minimum information security practices required, especially in the handling of Personal Data in which STIHL is the Controller, are

- Inform, without delay, if Personal Data or mobile storage media are lost, copied without authorization or obtained by espionage, as well as if there are indications of any other irregularities related to the treatment of Personal Data;
- Maintain adequate access controls, keeping access logs, with date, time and computer used for the access to said data, as well as record of activities performed and limiting access to Personal Data to what is strictly necessary to provide the services, also ensuring security, integrity, confidentiality and traceability of access to Data;
- Provide agents, employees and all employees with appropriate training on information security and Personal Data protection;
- The system should be protected by appropriate protection software, such as a virus scanner against cyber attacks. The protection software should be kept up-to-date at all times;
- The facilities that store the systems or parts must be protected by appropriate measures to prevent falsification of data, such as blocking and control systems against access by unauthorized persons, in particular if the system or parts are not under permanent visual control of the Supplier;
- Protect personal and confidential data to authorized persons by means of a user ID and a complex personal password that shall be changed at least every 180 days. If the system is also used by unauthorized persons, it is necessary to ensure that such persons cannot access the Personal Data;
- If the system is connected to the Internet or if the system can be accessed in any other way, an appropriately configured firewall or other appropriate measures should be used in order to prevent unauthorized external access to the system;
- If Data is stored and transported via mobile memory device such as memory cards, CDs or data processing devices like notebooks, they must be protected by strong encryption.

By entering into a business relationship as a STIHL Supplier, the Supplier agrees to be bound by this Privacy and Data Protection Policy for Suppliers.