AVS ELECTRONICS S.p.A.
a Socio Unico
Via Valsugana, 63 – 35010 Curtarolo (PD) Italy
Tel. 049 96 98 411 r.a. Fax 049 96 98 407
PEC: ammin.avs@legalmail.it
www.avselectronics.com - avs@avselectronics.it
Cap. Soc. €. 800.000,00 i.v.
Reg. Imprese PD 00381050285
R.E.A. Padova n. 121975
CF/P.IVA 00381050285

PRIVACY POLICY

INTRODUCTION

Data protection is an important commitment for AVS ELECTRONICS S.p.A. (hereinafter "**DATA CONTROLLER**" or "**Company**").
The entry into force of Regulation (EU) 2016/679 "*Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data*" (the "**GDPR**") has provided the opportunity for the Company's activities to be adapted further to the requirements for the transparency and protection of data protection, in accordance with the fundamental rights and freedoms of all data subjects whether they be employees, collaborators, customers, suppliers or third parties interested in receiving information.
AVS ELECTRONICS S.p.A. has therefore implemented an "Organisational Privacy Model" (OPM), which is outlined below, and the aim of which is to analyse all data processing operations, to organise them on a functional basis and to manage them securely and transparently. This section of the website also contains information about the rights of the data subject and the way in which these rights can be exercised towards the Data Controller.

CONTENTS

1 - GDPR ORGANISATIONAL PRIVACY MODEL

1.1 PARTIES

DATA CONTROLLER
The Data Controller is:
AVS ELECTRONICS S.p.A. (hereinafter also "**DATA CONTROLLER**")
Curtarolo (PD), Via Valsugana n. 63
Tel. +39 049 9698411
email: avs@avselectronics.it
Certified email address: ammin.avs@legalmail.it
VAT no. and tax code: 00381050285

DATA PROTECTION OFFICER
The Data Protection Officer is
TZ&A Studio Associato (hereinafter also "**DPO**")
email: dpo@avselectronics.it.

The DATA CONTROLLER has deemed it appropriate to appoint a Data Protection Officer (DPO) pursuant to Art. 37 of the EU Regulation 679/2016, which acts in synergy with the internal privacy team.

PRIVACY TEAM
The DATA CONTROLLER considered it appropriate to appoint an internal "Privacy Team" made up of internal and external subjects, with organizational, technical and IT skills.
The Privacy Team has the function of supporting the activity of the DATA CONTROLLER and DPO.

AUTHORISED DATA PROCESSORS (ex Art. 29 GDPR)
The OPM requires that every employee or person working on behalf of the DATA CONTROLLER only processes the data necessary to fulfil his or her duties based on the internal organisation and purposes indicated or proposed to the data subject ("limitation of purpose and minimisation of data", Art. 5(1) b) and c) GDPR). The processing operations have thus been segmented into sections of authorised data processors, with the employees/collaborators responsible for each section being restricted to a specific area of processing. Each authorised data processor has received specific instructions from the DATA CONTROLLER pertaining to the processing of personal data. The information system is also formed "watertight compartments", by design. Employees/collaborators may only access the data necessary to fulfil their duties, from their workstations. The allocation to specific data processing areas is based on a careful analysis of the company's structure and organisation, and the flow of internal and external data.
Employees/collaborators also receive internal regulations on the use of IT tools and on the rules of conduct and ethics pertaining to all the information they access in relation to their roles.
To ensure the effective adaptation to requirements concerning the processing of personal data, the Data Controller has also provided adequate training to its employees/collaborators, who process personal data in connection with their duties.

INTERNAL AND EXTERNAL SYSTEM ADMINISTRATORS
The DATA CONTROLLER uses information tools to manage and organise its activity. For this reason, the DATA CONTROLLER's activity is always underpinned by careful attention to the construction of software, the use of that software, and data security. Persons with "administrator" privileges within the company are specifically appointed and trained. The specialised external companies accessing internal data are also specifically appointed as External Data Processors and/or External System Administrators as defined in Article 28 of the GDPR.

Providers of external IT services are chosen with attention to their professionalism, not only in technical terms but also in relation to compliance with data protection requirements. Certified providers are preferred.

DATA PROCESSORS (ex Art. 28 GDPR)

In principle, the DATA CONTROLLER manages almost all the processing operations internally. The outsourcing to third parties of various activities that imply the processing of data on the DATA CONTROLLER's behalf are indicated in the individual policies, as appropriate. In these cases, relations with the third-party provider are governed by a specific "Data Processor" contract, as required by Article 28 of the GDPR.

The DATA CONTROLLER entrusts the processing operations to external providers who can offer sufficient guarantees of technical and organisational measures, in order to satisfy the requirements of the GDPR and to protect the rights of the data subjects.

1.2 RISK ANALYSIS AND MEASURES TO PREVENT DATA PROTECTION RISKS

According to the principle of "accountability", the DATA CONTROLLER is responsible for implementing a series of organisational, physical, legal, technical and information technology measures designed to prevent the risk of infringement of the data subject' personal rights and freedoms. In order to meet this objective, a regular risk analysis is conducted based on the processing operations, the tools used, and the type and volume of data processed.

RECORDS OF PROCESSING ACTIVITIES (Art. 30 GDPR) AND ANALYSIS OF IMPACT ON DATA PROTECTION (Art. 35 GDPR)

The OPM provides for a thorough, regular risk analysis in relation to data processing, for each activity or service provided, through a Record of processing activities (Article 30 (1) of the GDPR).

After analysing the processing activity performed by the DATA CONTROLLER, we consider that there are currently no risky activities that would require a specific impact assessment as defined in Article 35 of the GDPR ("DPIA").

The analysis of the information technology risks, and risks pertaining to company hardware and software, and the related adaptation measures, was carried out by our System Administrator using specific tools and checklists, and also by an external information security firm, which carried out an in-depth audit including security tests. The results of the audit enabled our technicians to further improve the measures used to protect against cyber-attacks and threats to information security. These were scaled in proportion to the risk to the rights and freedoms of the data subjects.

2 - TRANSPARENCY AND RIGHTS OF THE DATA SUBJECT

2.1 RIGHTS PERTAINING TO DATA PROTECTION

Also, in this area, the DATA CONTROLLER considers it essential to inform the data subjects of the existence of various rights pertaining to the protection of personal data. These are listed below.

- **Right to be informed (transparency in data processing)**

The data subject has the right to be informed about how the DATA CONTROLLER processes his or her personal data, for which purposes, and in relation to the other information provided for in Article 13 of the GDPR. For this purpose, the DATA CONTROLLER has put in place organisational processes that enable specific information forms to be issued whenever personal data is obtained or requested, depending on the category of data subject to which the interested party belongs (employee, customer, supplier etc.). This document enables adequate information to be provided to all data subjects, about how the DATA CONTROLLER processes their data. The information form can be requested by contacting the DATA CONTROLLER.

- **Right to revoke consent (Art. 13)**

You have the right to revoke consent at any time in relation to any processing operation that requires your prior consent. Revocation of consent does not affect the legitimacy of any previous data processing.

- **Right of access to data (Art. 15)**

You may request a) the purposes of the processing; b) the categories of personal data concerned; c) the recipients or categories of recipients to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations; d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period; e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing; f) the right to lodge a complaint with a supervisory authority; g) where the personal data are not collected from the data subject, any available information as to their source; h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4), and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject. You have the right to request a copy of the personal data that have been processed.

- **Right of rectification (Art. 16)**

You have the right to obtain the rectification of inaccurate personal data concerning you, and to have incomplete personal data completed.

- **Right to be forgotten (Art. 17)**

You have the right to obtain from the controller the erasure of personal data concerning you if the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; if you withdraw consent; if there are no overriding legitimate grounds for the processing, if there is a legal obligation to erase the data; if the data relates to online services provided to minors, without the related consent. The personal data may be erased unless there is an overriding right to the freedom of expression and of information, the personal data is kept in order to fulfil a legal obligation or to perform a duty carried out in the public interest or in the exercise of public powers, for reasons of public interest in the healthcare sector, for the purposes of archiving in the public interest, scientific research, historical research, for statistical purposes or to establish, exercise or defend a right in legal proceedings.

- **Right to restriction of processing (Art. 18)**

You have the right to obtain from the controller restriction of processing when you have contested the accuracy of the personal data (for a period enabling the controller to verify the accuracy of the personal data) or if the processing is unlawful but you oppose the erasure of the personal data and request the restriction of their use instead; or if they are necessary for the establishment, exercise or defence of a right in legal proceedings, while they are no longer necessary to the Data Controller.

- **Right to data portability (Art. 20)**

You have the right to receive, in a structured, commonly used and machine-readable format, the personal data concerning you which you have provided to us, and you also have the right to transmit those data to another controller if the processing is based on consent, on a contract, and if the processing is carried out by automated means, except where processing is necessary for the performance of a task carried out in the public interest or connected to the exercise of public powers, and the transmission does not adversely affect the rights of others.

- **Right to object (Art. 21)**

You have the right to object at any time to the processing of all or part of your personal data if the processing is carried out in the pursuit of a legitimate interest of the Data Controller or for the purposes of direct marketing.

- **Right to lodge a complaint with a Supervisory authority (Art. 77).**

Without prejudice to any other administrative or judicial remedy, if you consider that the processing of your personal data infringes the GDPR, you have the right to lodge a complaint with a supervisory authority, in particular in the Member State of your habitual residence, place of work, or place of the alleged infringement.

2.2 EXERCISING DATA PROTECTION RIGHTS

In order to exercise your rights, you may request information from the DATA CONTROLLER or complete the contact form, which we have provided to you below.

AVS ELECTRONICS S.p.A.
a Socio Unico
Via Valsugana, 63 – 35010 Curtarolo (PD) Italy
Tel. 049 96 98 411 r.a. Fax 049 96 98 407
PEC: ammin.avs@legalmail.it
www.avselectronics.com - avs@avselectronics.it
Cap. Soc. €. 800.000,00 i.v.
Reg. Imprese PD 00381050285
R.E.A. Padova n. 121975
CF/P.IVA 00381050285

2.3 FORMS AND POLICIES

1) Forms - Below is a draft document which you should print out and complete, in order to exercise your rights as data subject, stating which right you wish to exercise. The form may be sent to the DATA CONTROLLER at the above addresses, in accordance with the current laws.

Link: Exercising data protection rights

2) Policies:

Link: Information for customers and suppliers
Link: Newsletter Marketing policy
Link: Information for job applicants
Link: Information for market research and customer satisfaction