

Privacy Policy on the processing of personal data of Suppliers pursuant to art. 13 of the GDPR

Pursuant to the current legislation on the protection of personal data (the "**Privacy Regulations**") including the EU Regulation 2016/679 (the "**GDPR**"), as well as Italian Legislative Decree 196/2003 as amended by Italian Legislative Decree 101/2018, **Geico S.p.A.**, in its capacity as data controller (the "**Company**" or the "**Data Controller**"), informs the representatives of suppliers (hereinafter also referred to as the "**Data Subjects**" or "**Suppliers**", or in the singular the "**Data Subject**" or the "**Supplier**") that within the scope of the supply contract existing between them and the Company (hereinafter, the "**Contract**"), the personal data referred to the Data Subjects will be processed in strict compliance with the Privacy Regulations, for the purposes and in the manner described in this policy (the "**Privacy Policy**").

1. WHO IS THE DATA CONTROLLER?

The Data Controller is Geico S.p.A., with registered office at Via Pelizza da Volpedo 109/111, Cinisello Balsamo (MI), 20092, Italy, VAT No. 00688580968, which can be contacted via the phone number +39 02 660221 or at the following e-mail address infoprivacy@geico-spa.com.

2. WHAT TYPE OF PERSONAL DATA WILL BE COLLECTED?

The Data Controller processes the following personal data collected during the conclusion and execution of the Contract:

- **identification and contact data of the Supplier**, obtained during contractual or pre-contractual relations with the Company, such as: name, address or other elements for personal identification; telephone and e-mail contact data; company name where containing personal data; data common to employees and/or collaborators and/or consultants of the Supplier;
- **data related to the professional career**, such as: education qualification; professional title;
- **financial and fiscal data**, such as: IBAN; current account number and, in general, the information needed to make payments and invoices.

3. FOR WHAT PURPOSES WILL PERSONAL DATA BE PROCESSED AND ON WHAT LEGAL BASIS WILL SUCH PROCESSING TAKE PLACE?

The Data Controller informs the Data Subjects that the personal data collected by the Company under the Contract, will be processed, through automated and manual methods, for the following purposes (the "**Purposes**"):

Purpose of the processing	Legal basis of data processing	Nature of personal data provision
a) Execution of the Contract and/or pre-contractual measures such as the selection of Suppliers, the negotiation of contractual relationships, the formalisation, conclusion and execution of the Contract, as well as the performance of activities related to the management of accounting and related obligations, contractual obligations, services, invoicing/payments, auditing and compulsory/optional certification of financial statements, assignment or advancement of receivables, as well as the fulfilment of specific requests and comply with other obligations under the Contract.	Art. 6(1)(b) of the GDPR: execution of the Contract to which the Data Subject is a party and execution of pre-contractual measures taken at the request of the Data Subject.	The provision of personal data is necessary for the establishment and proper conduct of the Contract, as well as to properly comply with the regulations in force and fulfil the obligations under the Contract. Therefore, any refusal by the Data Subject to provide personal data, in whole or in part, for the fulfilment of the aforementioned Purposes, will make it impossible to establish or execute the Contract or to properly fulfil the obligations required by the regulations in force.

<p>b) Fulfilment of the obligations provided for by the law, regulations, Community legislation or an order from the Authority (for example, accounting and budgetary obligations, anti-money laundering, antitrust, as well as obligations relating to customs, tax, healthcare, labour and safety, etc.).</p>	<p>Art. 6(1)(c) of the GDPR: legal obligation to which the Data Controller is subject.</p>	
<p>c) Management of the fulfilments related to the internal corporate and financial organisation (e.g. company secretariat, communications, deposits, reports, etc.), as well as internal reporting & controlling of the Company.</p>	<p>Art. 6(1)(f) of the GDPR: legitimate interest of the Data Controller to the proper management of the company in relation to accounting and financial organisation.</p>	
<p>d) Organisation and management of corporate events in which Suppliers take part, aimed at strengthening the corporate identity of the Company.</p>	<p>Art. 6(1)(f) of the GDPR: legitimate interest of the Data Controller in promoting Geico's image externally, thus strengthening its corporate identity.</p>	
<p>e) Verification, exercising or protection of a right during a judicial proceeding.</p>	<p>Art. 6(1)(f) of the GDPR: legitimate interest of the Data Controller relating to the right to defend and exercise its rights or those of a third party.</p>	
<p>f) Transmit personal data within the business group for internal administrative purposes, including the processing of customer or employee personal data.</p>	<p>Art. 6(1)(f) of the GDPR: legitimate interest of the Data Controller to the correct internal administrative management. NOTE The legitimate interest as a legal basis for intra-group transfers of personal data is only appropriate for transfers between Group companies located within the European Economic Area. If the intent of the Data Controller is to transfer personal data to other companies of the Group located in non-EU countries, please refer to Paragraph 6 of this Privacy Policy.</p>	
<p>g) Use of the professional photo of the Data Subject, where the Company's customers require a more detailed organisation chart of the individuals who will be involved in the project (therefore, including Suppliers).</p>	<p>Art. 6(1)(a) of the GDPR: explicit consent of the Data Subject.</p>	<p>The provision of personal data for the indicated purpose is optional and data can only be processed after the Data Subject's consent. Failure to consent to this Purpose will have the sole consequence of preventing the processing of personal data by the Data Controller for this specific Purpose.</p>

If the legal basis of the processing is the legitimate interest of the Data Controller, the latter guarantees to have previously carried out an assessment aimed at ensuring the **proportionality of the processing** so that the rights and freedoms of the Data Subjects are not prejudiced, taking into account the reasonable expectations of the same in relation to the specific processing activity carried out.

Data Subjects may request **additional information about the above assessment** by sending an email to the following address: [infoprivacy@geico-spa.com].

The Data Controller also informs the Data Subject that s/he has the right to (i) **revoke**, at any time, any consent given, it being understood that the revocation of consent shall not affect the lawfulness of the processing based on consent prior to revocation; (ii) **object** to the processing of their personal data based on the legitimate interest of the Company.

If the Company intends to use the personal data for any other purpose that is incompatible with the Purposes for which they were originally collected or authorised, the Company will inform the Data Subject in advance and, when required, will request consent for further processing of the data.

4. HOW WILL PERSONAL DATA BE PROCESSED?

In relation to the indicated Purposes, the processing of Personal Data may consist of the activities indicated in Article 4, paragraph 1, no. 2) of the GDPR, namely: collection, recording, organisation, storage, consultation, processing, disclosure by transmission, or otherwise making available, restriction, erasure or destruction of Personal Data.

In addition, the personal data of the Data Subjects will be:

- processed in compliance with the principles of **lawfulness, correctness and transparency**;
- collected for the **legitimate Purposes** determined above;
- **adequate, relevant and limited** to the Purposes for which they are processed;
- **stored in a form that allows the identification of the Data Subject for a period of time not exceeding the fulfilment of the purposes** and better defined in point 7 below;
- processed in such a way as to guarantee **adequate security against the risk of destruction, loss, modification, disclosure or unauthorised access by means of technical and organisational security measures**.

Data can be processed through manual, automated, IT and telematic means, according to a logic strictly related to the purposes and, however, in such a way as to ensure the security and confidentiality of data, in addition to compliance with the specific obligations under the Privacy Regulations in force and applicable from time to time.

5. TO WHOM WILL PERSONAL DATA BE DISCLOSED?

The personal data of the Data Subjects will be processed by the Company's employees, who will be specifically designated as **authorised subjects**, where processing is required for the fulfilment of the Purposes set out in point 3 of this Privacy Policy.

Furthermore, the Data Controller informs the Suppliers that, for the fulfilment of the Purposes, their personal data may be disclosed to **further recipients or categories of recipients**, in their capacity as autonomous data controllers or, where necessary, specially appointed data processors, including, by way of example but not limited to:

- Banks
- insurance companies;
- consultants and freelancers as individuals or in associated form (accountants and accounting experts, auditors, lawyers), both Italian and foreign;
- debt collection companies;
- companies that detect financial risks and carry out fraud prevention activities;
- public administrations and supervisory and control Authorities, both Italian and foreign;
- companies that provide IT services;
- parent companies and/or associated companies of the Company;
- Customer companies of the Data Controller.

The complete list of the recipients of the personal data of the Data Subjects, including further details on the location of the recipients, is kept at the Data Controller's head office and can be consulted upon request to be sent to the addresses indicated in point 8 of this Privacy Policy.

Finally, the Data Controller informs the Data Subjects that their **personal data will not be disclosed to third parties and will not be disseminated**.

6. ARE PERSONAL DATA TRANSFERRED TO COUNTRIES OUTSIDE THE EU?

As part of an **international group**, Geico informs the Data Subjects that, in order to process the personal data for the Purposes set forth in point 3 above of this Privacy Policy, some personal data may be transferred to companies of the Geico group having their registered offices **outside the European Union** (the countries include: **Japan, Russia, Brazil, China, India, Mexico, United Kingdom, United States of America**).

Considering that some of the aforementioned countries do not guarantee an adequate level of protection of personal data compared to that provided in the European Union, the Data Controller has taken steps to ensure that the transfer of the personal data of the Data Subjects to such countries takes place solely in compliance with the conditions set forth in Articles 45/49 of the GDPR and, in particular:

- in Japan: [COMMISSION IMPLEMENTING DECISION \(EU\) 2019/419 of 23 January 2019](#);
- in the United Kingdom: [COMMISSION IMPLEMENTING DECISION \(EU\) 2021/915 of 04 June 2021](#);

Where the Company intends to transfer the personal data of Employees to non-EU countries other than those mentioned above, such transfer shall take place only in accordance with the conditions set out in Articles 45/49 of the GDPR.

7. HOW LONG WILL PERSONAL DATA BE RETAINED?

The personal data of the Data Subjects necessary for the conclusion and execution of the Contract will be retained and processed for the entire duration of the Contract and, following its termination, for whatever reason, for a period not exceeding 10 years (i.e. the ordinary limitation period), with reference to the data necessary for the issue of certificates or documentation that may be required for any legal, fiscal and accounting obligations connected with or arising from the termination of the Contract, as well as for the legal protection of the Company.

Images of Data Subjects will be retained for a period of 24 months, without prejudice to Data Subjects' right to revoke their previous consent to the processing of such personal data.

At the end of the retention period, personal data of Data Subjects will be deleted, unless there are further legitimate interests of the Data Controller and/or legal obligations that make it necessary to retain it, after minimisation.

8. WHAT ARE YOUR RIGHTS IN RELATION TO THE PROCESSING OF YOUR PERSONAL DATA, HOW CAN YOU EXERCISE THEM AND HOW CAN YOU CONTACT US?

The Data Controller informs the Data Subject that s/he will always have, in accordance with the law, the right to revoke at any time his/her consent, where given, as well as to exercise, at any time, the following rights (collectively, the "**Rights**"):

- a) the "**right of access**" and specifically to obtain confirmation of the existence or otherwise of personal data concerning him or her and their communication in intelligible form;
- b) the "**right to rectification**", i.e. the right to request the rectification or, if interested, the integration of personal data;
- c) the "**right to erasure**", i.e. the right to request the erasure, transformation into anonymous form of data processed in violation of the law, including data whose storage is not necessary in relation to the purposes for which the personal data were collected or subsequently processed;
- d) the "**right to restriction of processing**", i.e. the right to obtain from the Data Controller the restriction of data processing in certain cases provided for under the Privacy Regulations;

- e) the right to request from the Data Controller the list of the recipients to whom any rectification or erasure or restriction of processing was notified (in accordance with Articles 16, 17 and 18 GDPR, in fulfilment of the notification obligation except where this proves impossible or involves a disproportionate effort);
- f) the "**right to data portability**", i.e. the right to receive (or to transmit directly to another data controller) personal data in a structured, commonly used and machine-readable format;
- g) the "**right to object**" i.e. the right to object, in whole or in part:
 - to the processing of personal data carried out by the Data Controller for its own legitimate interest;
 - to the processing of personal data carried out by the Data Controller for marketing or profiling purposes.

In the above cases, where necessary, the Data Controller will inform the third parties to whom the Data Subject's personal data are communicated of the possible exercise of rights, except in specific cases where this is not possible or is too costly and, in any case, in accordance with the provisions of the Privacy Regulations.

The Data Subject may at any time exercise his/her Rights in the following ways:

- by email sent to: infoprivacy@geico-spa.com;
- by ordinary mail, to the address of the registered office of Geico S.p.A.: Cinisello Balsamo (MI), Via Pelizza da Volpedo 109/111, 20092, Italy.

9. HOW CAN YOU LODGE A COMPLAINT WITH THE ITALIAN AUTHORITY ("GARANTE")?

The Data Controller informs the Data Subject that, pursuant to the Privacy Regulations, he or she has the right to lodge a complaint with the competent supervisory Authority (in particular in the Member State of his or her usual residence, place of work or place of the alleged breach), if he or she deems that his or her Personal Data are being processed in a manner that would result in a breach of the GDPR.

In order to facilitate the exercise of the right to lodge a complaint, the name and contact details of the European Union Supervisory Authorities are available at the following link https://ec.europa.eu/justice/article-29/structure/data-protection-authorities/index_en.htm.

Finally, if the Data Subject intends to lodge a complaint with the Supervisory Authority competent for the Italian territory (i.e. Italian Data Protection Authority ("Garante")), the complaint form is available at the following link: <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/4535524>.

Data subject consent request form

Having read and understood the above Privacy Policy on the processing of personal data

I consent

I do not consent

to the processing of my personal data (i.e. my photograph), for the Purpose referred to in Paragraph 3, letter g), i.e. for the use of my professional photograph, where Geico's customers require a more detailed organisation chart of the persons who will participate in the project.

[place and date]

Signature _____

NOTE The consent to the processing of personal data may be revoked at any time by sending an email to the following address: [\[infoprivacy@geico-spa.com\]](mailto:infoprivacy@geico-spa.com).

However, revocation of previously given consent does not affect the lawfulness of processing based on consent prior to revocation.