

**Allied Group** considers personal data as a primary asset to be protected, adopting procedures and behaviors aimed to ensure their security and confidentiality.

**Transparency to data subjects** is therefore a primary objective, pursued through effective communication tools. The company takes appropriate measures to provide any information relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form (GDPR, Art.12).

In this regard, this information page, created according to the requirements of the EU Reg. 2016/679 "General Data Protection Regulation", contains specific information relating to the following areas:

- 1) GENERAL INFORMATION (compliance profiles applicable to all processing carried out by Group companies);
- 2) DATA PROCESSING RELATED TO RELATIONS WITH CUSTOMERS AND SUPPLIERS (compliance profiles applicable to processing in the administrative / operational / commercial area)
- 3) DATA PROCESSING RELATED TO THE WEBSITE (compliance profiles connected to navigation data and cookies)
- 4) DATA PROCESSING CONNECTED TO VIDEO SURVEILLANCE SYSTEMS (compliance profiles connected to the offices where security cameras are operating)
- 5) COMPLIANCE WITH EXTRA-UE REGULATIONS
- 6) POLICY UPDATING.

This policy may in any case be supplemented, if necessary, by specific information provided to the interested parties in the manner permitted by current regulations.

## **1. GENERAL INFORMATION**

### **1.1 General processing profiles**

We inform data subject (Art.4, c.1 del GDPR) about the following general items:

- personal data are processed according to current privacy regulation (Reg.UE 2016/679 "GDPR" and D.Lgs.196/2003 as integrated by D.Lgs.101/2018)
- personal data are processed lawfully, fairly and in a transparent manner, according to principles of GDPR, Art.5;
- specific security measures are implemented to prevent the data from being lost, used unlawfully and/or inappropriately, and accessed without authorization, according to principles of GDPR, Art.32.

### **1.2 Data Controller and contacts**

The Data Controller is each company of the Group, as regards the data processing carried out with its stakeholders. A complete list of the Data Controller companies and their contact details is available on the website: <https://www.allied-group.com/template.php?rpage=home&l=it> (from this section it is possible to access to the website of each individual company and related contacts).

It should also be noted that it is possible to contact the Data Protection Officer by writing to: [dpo@gallidataservice.com](mailto:dpo@gallidataservice.com)

### **1.3 Rights of the data subject**

It is possible to contact the Data Controller or the DPO to exercise the rights referred to in Articles 15-22 of the GDPR:

- the right to request the presence and access to personal data (Art.15 "Right of access")
- the right to obtain the correction / integration of incorrect or incomplete data (Art.16 "Right of rectification")
- the right to obtain, if there are justified reasons, the cancellation of data (Art.17 "Right to cancel")
- the right to obtain the processing limitation (Art.18 "Right to limitation")
- the right to receive data in a structured format (Art.20 "Right to portability")
- the right to oppose the processing and automated decision-making processes, including profiling (Art.21, 22)
- the right to revoke a previously granted consent;
- right to present, in case of non-reply, a complaint to the Data Protection Authority.

## **2. DATA PROCESSING CONNECTED TO THE RELATIONSHIPS WITH CUSTOMERS AND SUPPLIERS**

### **2.1 Object of the processing**

The Company processes personal identifying data of customers / suppliers (for example, name, surname, company name, personal / fiscal data, address, telephone, e-mail, bank and payment details) and its operative contacts (name surname and data contact information) acquired and used for managing the products/services provided by the Company.

### **2.2 Purposes and legal basis of the processing**

Data are processed to:

- conclude contractual / professional relationships;
- fulfill the pre-contractual, contractual and tax obligations deriving from existing relationships, as well as manage the necessary communications connected to them;
- fulfill the obligations established by law, by a regulation, by community legislation or by an order of the Authority;
- exercise a legitimate interest as well as a right of the Data Controller (for example: the right of defense in court, the protection of credit positions; the ordinary internal needs of an operational, managerial and accounting nature).

Failure to provide the aforementioned data will make it impossible to establish the relationship with the Controller. The aforementioned purposes represent, pursuant to Article 6, commi b, c, f, suitable legal bases for the lawfulness of the processing. If it is intended to carry out treatments for different purposes, it will be required a specific consent from the data subjects.

### **2.3 Methods of the processing**

The processing of personal data is carried out by means of the operations indicated in Art. 4 n. 2) GDPR and exactly as: collection, registration, organization, storage, consultation, processing, modification, selection, extraction, comparison, use, interconnection, blocking, communication, deletion and destruction of data. Personal data are subjected to both paper and electronic and / or automated processing. The Data Controller will process personal data for the time necessary to fulfill the purposes for which it was collected and related legal obligations.

### **2.4 Scope of the processing**

The data are processed by internal regularly authorized subjects and instructed pursuant to Article 29 of the GDPR. It is also possible to request the scope of communication of personal data, obtaining precise indications on any external subjects operating as managers or independent data controllers (consultants, technicians, banks, transporters, etc.). We wish to make you aware of personal data may be the subject of intercompany communication between Group companies. The data are not subject to disclosure or transfer outside the EU (they may be transferred outside the EU only in compliance with the conditions set out in Chapter V of the GDPR, aimed at ensuring that the level of protection of the data subjects is not compromised "Article 45 Transfer on the basis of an adequacy decision, Article 46 Transfer subject to adequate guarantees, Article 47 Binding corporate rules, Article 49 Specific exceptions "). The data are not subject to automated processes that produce significant consequences for the data subject.

## **3. DATA PROCESSING RELATED TO THIS WEBSITE**

### **3.1 Navigation Data**

The information systems and software procedures relied upon to operate this web site acquire personal data as part of their standard functioning; the transmission of such data is an inherent feature of Internet communication protocols. Such information is not collected in order to relate it to identified data subjects, however it might allow user identification after being processed and matched with data held by third parties. This data category includes IP addresses and/or the domain names of the computers used by any user connecting with this web site, the URI (Uniform Resource Identifier) addresses of the requested resources, the time of such requests, the method used for submitting

a given request to the server, returned file size, a numerical code relating to server response status (successfully performed, error, etc.), and other parameters related to the user's operating system and computer environment.

<b>Purposes and lawfulness of processing</b> (GDPR-Art.13, c.1, lett.c)	These data are only used to extract anonymous statistical information on website use as well as to check its functioning. The data might be used to establish liability in case computer crimes are committed against the website (Controller legitimate interest).
<b>Scope of communication</b> (GDPR-Art.13, c.1, lett.e,f)	The data may only be processed by internal personnel, duly authorized and instructed in the processing (GDPR-Art.29) or by the Processor of the web platform (appointed Data Processor, Art.28 GDPR) and will not be disclosed to other parties, disseminated or transferred to non-EU countries. Only in the case of an investigation they can be made available to the competent authorities.
<b>Data retention</b> (GDPR-Art.13, c.2, lett.a)	Data are usually kept for short periods of time, with the exception of any extensions connected to investigations.
<b>Data provision</b> (GDPR-Art.13, c.2, lett.f)	The data are not provided by the data subject but automatically acquired by the site's technological systems.

**3.2 Cookies**

The management of cookies is consistent with the regulatory requirements on the subject:

- "Guidelines for cookies and other tracking tools" of 10 June 2021 (Published in the Official Gazette no. 163 of 9 July 2021);
- Guidelines 5/2020 on consent pursuant to Reg. (EU) 2016/679, adopted by the European Data Protection Board.

The user can check the types of cookies and set their preferences through the appropriate banner (if applicable), as well as through the appropriate tools provided by the main browsers. Below is some general information about cookies and similar technologies.

**What are cookies:** Cookies are short fragments of text (letters and / or numbers) that allow the web server to store on the client (the browser) information to be reused during the same visit to the site (session cookies) or later , even after days (persistent cookies). Cookies are stored, according to user preferences, by the single browser on the specific device used (computer, tablet, smartphone). Similar technologies, such as, for example, web beacons, transparent GIFs and all forms of local storage introduced with HTML5, can be used to gather information on user behavior and use of services. In the continuation of this information we will refer to cookies and all similar technologies simply by using the term "cookies".

**Possible types of first-party cookies and how to manage preferences**

CATEGORY	AIM	MANAGEMENT
<b>Technical and session cookies</b>	Ensure normal navigation and use of the site	Through the main browsers you can: <ul style="list-style-type: none"> <li>• Block by default the reception of all (or some) types of cookies</li> <li>• View the analytical list of the cookies used</li> <li>• Remove all or some of the installed cookies</li> </ul> For information on setting individual browsers see specific paragraph. It should be noted that blocking or deleting cookies could compromise the navigability of the site.
<b>Analytics</b>	Collect information on the number of visitors and on the pages viewed	
<b>Profyling</b>	Create profiles related to the user in order to send advertising messages in line with the preferences	

The site may contain links to third-party sites and third-party cookies; for more information, we invite you to view the privacy policy of any linked sites.

**Management of preferences through the main browsers** The user can decide whether or not to accept cookies using the settings of their browser (we point out that, by default, almost all web browsers are set to automatically accept cookies). The setting can be modified and defined specifically for different websites and web applications. In addition, the best browsers allow you to define different settings for cookies "owners" and those of "third parties". Usually, cookies are set up from the "Preferences", "Tools" or "Options" menu.

Below are links to the guides for managing cookies from the main browsers:

**Internet Explorer:**<http://support.microsoft.com/kb/278835>

**Internet Explorer [versione mobile]:** <http://www.windowsphone.com/en-us/how-to/wp7/web/changing-privacy-and-other-browser-settings>

**Chrome:**<http://support.google.com/chrome/bin/answer.py?hl=en-GB&answer=95647>

**Safari:**<http://docs.info.apple.com/article.html?path=Safari/5.0/en/9277.html>

**Safari [versione mobile]:** <http://support.apple.com/kb/HT1677>

**Firefox:**<http://support.mozilla.org/en-US/kb/Enabling%20and%20disabling%20cookies>

**Android:**<http://support.google.com/mobile/bin/answer.py?hl=en&answer=169022>

**Opera:**<http://help.opera.com/opera/Windows/1781/it/controlPages.html#manageCookies>

#### Further information

- [www.allaboutcookies.org](http://www.allaboutcookies.org) (for more information on cookies technologies and their operation)
- [www.youronlinechoices.com/it/a-proposito](http://www.youronlinechoices.com/it/a-proposito) (allows users to oppose the installation of the main profiling cookies)
- [www.garanteprivacy.it/cookie](http://www.garanteprivacy.it/cookie) (collection of the main regulatory measures on the matter by the Italian Guarantor Authority)

#### 3.3 Specific services

The website may contain data collection forms designed to guarantee the user any services / features (eg: request information, registrations, work with us, etc.).

<b>Purpose and legal basis of the processing</b> (GDPR-Art.13, comma 1, lett.c)	The identification and contact data necessary to respond to the requests of the data subjects could be requested. The submission of the request is subject to specific, free and informed consent (GDPR-Art.6, comma1, lett.a).
<b>Scope of communication</b> (GDPR-Art.13, paragraph 1, lett.e, f)	The data are processed exclusively by authorized and trained personnel (GDPR-Art.29) or by any persons responsible for maintaining the web platform or providing of the service (appointed in this case external managers). The data will not be disclosed or transferred to non-EU countries.
<b>Data retention period</b> (GDPR-Art.13, paragraph 2, letter a)	Data are kept for times compatible with the purpose of the collection.
<b>Data provision</b> (GDPR-Art.13, comma 2, lett.f)	The provision of data related to the mandatory fields is necessary to obtain an answer, while the optional fields are aimed at providing the staff with other useful elements to facilitate contact.

#### 3.4 Data provided voluntarily by the user

The optional, explicit and voluntary sending of messages to contact addresses, private messages sent by users to institutional profiles / pages on social media (where this possibility is foreseen), as well as the compilation and forwarding of any forms / modules present, involve the acquisition of the sender's contact data, necessary to reply, as well as all personal data included in communications.

The sender therefore remains personally responsible for the accuracy of the data provided, as well as for their relevance and not excess with respect to the requests in question.

#### **4. DATA PROCESSING CONNECTED TO VIDEO SURVEILLANCE SYSTEMS**

We inform you that video surveillance systems may be in operation at some offices of the companies of the Group (duly indicated by means of special "VIDEO SURVEILLED AREA" signs). The processing of personal data through video surveillance systems takes place in compliance with current privacy regulations (EU Reg. 2016/679 "GDPR"; Legislative Decree 196/2003, as amended and supplemented by Legislative Decree 101/2018 ; General Provisions of the Guarantor Authority for the protection of personal data, expressly recognized by Article 22, paragraph 4 of Legislative Decree 101/2018). The systems are installed for SECURITY purposes and the use of the cameras is aimed at protecting assets, people and assets against possible intrusions, fires, thefts, robberies or acts of vandalism and the possible defense of the rights of the owner in court. (evidence acquisition). The images detected can be recorded and stored for the period of time strictly necessary to achieve the aforementioned purpose, and in any case for a time not exceeding the terms established by law (never exceeding 7 days), except for any longer term necessary. to fulfill specific requests of the judicial authority or judicial police in relation to ongoing investigative activities; at the end of the envisaged retention period, the recorded images are deleted from their electronic, computer or magnetic media. The images can only be processed by formally authorized and trained personnel or by external companies who, as data processors, collaborate in the maintenance of the systems and in the surveillance activities; they are in no way communicated or disseminated outside the owner's structure, without prejudice to the execution of any orders from the judicial authorities or the judicial police or, in the case of offenses, use in any judicial offices. The images will be treated with suitable tools and methods to ensure an adequate level of security and confidentiality, with particular reference to the measures indicated in Article 32 of the GDPR and General Provision of 08/04/2010. Any filming of workers and use of videotaped images takes place in compliance with current regulations on labor law (Art. 4 L.300 / 70 "Workers' Statute", as amended by Art. 23 of Legislative Decree 151 / 2015 "latest implementing decree Jobs Act").

#### **5. COMPLIANCE WITH EXTRA-UE REGULATIONS**

##### **DO NOT TRACK**

##### **What is DNT?**

DNT is a concept promoted by regulators, particularly the US Federal Trade Commission (FTC), for industries to develop and implement a mechanism to allow Internet users to control the tracking of their online activities on websites.

##### **What does the rule provide?**

On September 27, 2013, the governor of California signed AB 370, which amends the California Online Privacy Protection Act (CalOPPA) to require website operators to disclose whether they honor browser "Do Not Track" settings related to advertising targeted and to reveal how they respond to DNT signals.

##### **How is compliance ensured?**

The Allied Group takes your privacy and security very seriously and is committed to putting you first in all aspects of our business. Therefore, Allied Group does not track its customers over time and across third-party websites to provide targeted advertising and therefore does not respond to Do Not Track (DNT) signals.

##### **PRIVACY AND MINORS**

The Children's Online Privacy Protection Act (COPPA) is a United States federal law that was put in place to better protect the personal data and rights of children under 13. Under COPPA, operators of websites or online services that target children under the age of 13 (or who have knowledge of collecting personal information from children under 13) must notify parents and obtain their verifiable consent before collect, use or disclose such information and must keep safe the information of children they collect. The use of this site is not intended for children under 18 years of age. The Allied Group will not knowingly collect personal data from minors through this site.

#### **6. POLICY UPDATING**

It should be noted that this information may be subject to periodic review, also in relation to the relevant legislation and jurisprudence. In the event of significant changes, appropriate evidence will be given in the home-page of the site for a suitable time. In any case, the interested party is invited to periodically consult the present policy.