

Imagicle Data Processing Addendum

How Imagicle processes personal and special data and what tools it provides to ensure its operations are GDPR-compliant

Updated on Oct, 2024

Imagicle spa

Via Fondacci, 272
55054 Massarosa
(LU) Italy

T +39.0584.943232
F +39.0584.943325
E info@imagicle.com
W www.imagicle.com

€ 353.080,00 paid up cap.
VAT ID IT 01715870463
company reg. 01715870463

a company part of Zucchetti spa

1 Purpose of the document

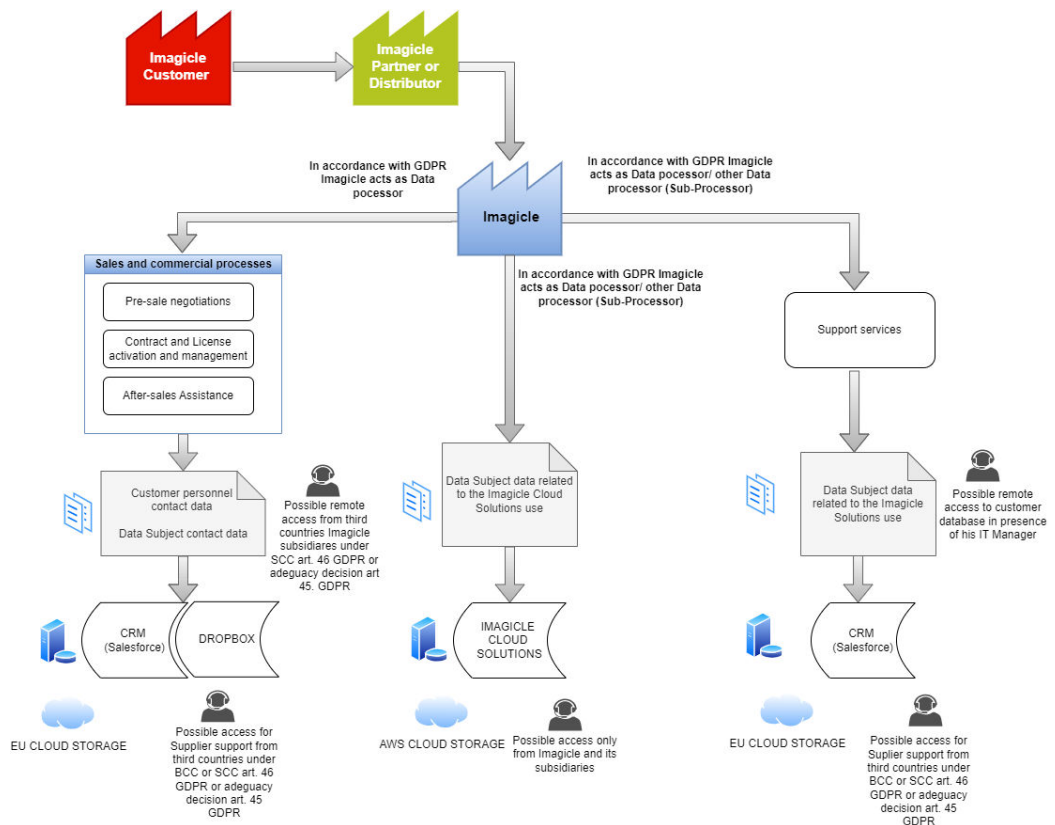
This document describes Imagicle processing of personal data, and it is prepared for courtesy purposes, to allow the Data Controller (Imagicle customer/partner/distributor providing Imagicle Solutions for use to the customer end-user) to have all the information needed to prepare the relevant privacy policies.

Imagicle will process personal data consistent with this Data Processing Addendum.

Concerning the processing of personal data processed in the context of the Customer's use of its Imagicle products and in the context of the provision of related services, Imagicle will act as a Data Processor if the Customer acts as a Data Controller and will act as a Sub-Processor (or other Sub-Processor) if the Customer acts as a Data Processor (or Sub-Processor).

2 What categories of data does Imagicle process?

Based on the provisions of the GDPR, "personal data" means any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly, with particular reference to an identifier such as a name, an identification number, location data, an online identifier, or one or more characteristic elements of his or her physical, physiological, genetic, mental, economic, cultural, or social identity.



Imagicle acts as *Data Processor* and may process such data for the following purposes:

- accessing data stored on the Customer's server/cloud with exclusive reference to the specific product activated for possible access during service and support
- proceeding to the creation of statistics and archives of resolved cases for analysis aimed at improving services (regarding user contact information only)
- sending communications related to contracted products/services and/or products/services similar to those already contracted (newsletters, webinars, training activities, product feature updates, etc.), with reference only to the contact details of the End Users of the product

The types of data processed depend on the specific product used, as further detailed in the table below:

LIST OF PERSONAL DATA PROCESSED FOR THE SPECIFIC UCX SUITE PRODUCT	
Attendant Console / Agent Console	<ul style="list-style-type: none"> • internal user information (Name, User, Password, First name, Last name, E-mail, Mobile number, Address, Office phone number) • internal user password only if local authentication is used • call-related data (Internal User's first and last name, Office phone number, external caller/caller number and related data loaded to the company address book, Area of origin, call duration data, call entry time and call transfers, user status and availability)
Advanced Queueing and Auto Attendant	<ul style="list-style-type: none"> • internal user information (Name, User, Password, First name, Last name, E-mail, Mobile number, Address, Office phone number) • internal user password only if local authentication is used • call-related data (Internal User's first and last name, Office phone number, external caller/caller number and related data loaded to the company address book, Area of origin, call duration data, call entry time and call transfers, user status and availability)
Call Recording	<ul style="list-style-type: none"> • internal user information (Name, User, Password, First name, Last name, E-mail, Mobile number, Address, Office phone number) • internal user password only if local authentication is used • call-related data (Internal User's first and last name, Office phone number, external caller/caller number and related data loaded to the company address book, Area of origin, call duration data) • call content (the content of the recorded calls can be about anything, also including health information and sensitive data)
Contact Manager	<ul style="list-style-type: none"> • internal user information (Name, User, Password, First name, Last name, E-mail, Mobile number, Address, Office phone number) • internal user password only if local authentication is used • external user information (First name, Last name, E-mail, Office extension number and/or cell phone number, Company)
Call Analytics	<ul style="list-style-type: none"> • internal user information (Name, User, Password, First name, Last name, E-mail, Mobile number, Address, Office phone number) • internal user password only if local authentication is used • data on incoming and outgoing telephone traffic (Internal User's first and last name, Office phone number, external caller/caller number and related data loaded to the company address book, Area of origin, call duration data)
Digital Fax	<ul style="list-style-type: none"> • internal user information (Name, User, Password, First name, Last name, E-mail, Mobile number, Address, Office phone number) • internal user password only if local authentication is used

	<ul style="list-style-type: none"> • fax related information (external number, Recipient name, Recipient number, time, date, source area) • content of faxes (The content of faxes can be about anything also including health information and sensitive data)
Hotel Services	<ul style="list-style-type: none"> • internal user information (Name, User, Password, First name, Last name, E-mail, Mobile number, Address, Office phone number) • internal user password only if local authentication is used information regarding the guest (First Name, Last Name) • call-related information (Guest's full name, Room number, Caller/caller number, area of origin) • contents of voicemail (Guest's first and last name. The contents of voicemail can, by its nature, be about anything, so it is possible that sensitive information may be in it)
Manager Assistant	<ul style="list-style-type: none"> • internal user information (Name, User, Password, First name, Last name, E-mail, Mobile number, Address, Office phone number) • internal user password only if local authentication is used • call-related data (Internal User's first and last name, Office phone number, caller/caller number and related data loaded to the personal address book, Area of origin, call duration data, call entry time and call transfers, user status and availability)
Screen Recording	<ul style="list-style-type: none"> • internal user information (Name, User, Password, First name, Last name, E-mail, Mobile number, Address, Office phone number) • internal user password only if local authentication is used • screen recorded content (the content recorded on the screen can be about anything happened during the agent conversation, also including health information and sensitive data treated during the call & screen recording session)
Voice Analytics	<ul style="list-style-type: none"> • internal user information (Name, User, Password, First name, Last name, E-mail, Mobile number, Address, Office phone number) • internal user password only if local authentication is used • call-related data (Internal User's first and last name, Office phone number, external caller/caller number and related data loaded to the company address book, Area of origin, call duration data) • call content (the content of the recorded calls can be about anything, also including health information and sensitive data)
Virtual Receptionist	<ul style="list-style-type: none"> • internal user information (Name, User, Password, First name, Last name, E-mail, Mobile number, Address, Office phone number) • internal user password only if local authentication is used • call-related data (Internal User's first and last name, Office phone number, external caller/caller number and related data loaded to the company address book, Area of origin, call duration data) • call content (the content of the transcribed and analyzed calls can be about anything, also including health information and sensitive data)
Smartflows Virtual Agents	<ul style="list-style-type: none"> • internal user information (Name, User, Password, First name, Last name, E-mail, Mobile number, Address, Office phone number) • internal user password only if local authentication is used • call-related data (Internal User's first and last name, Office phone number, caller/caller number and related data loaded to the company address book, Area of origin, call duration data, call entry time and call transfers, user status and availability) • chat-related data (Internal User's first and last name, Office phone number, email and/or caller number, IP Address of origin, chat start time, user status and availability) • chat-content (the content of the chat can be about anything, also including health information and sensitive data) • call content (the content of the transcribed and analyzed calls can be about anything, also including health information and sensitive data)

3 Who handles the Data?

- Imagicle Employees in Charge of Processing
- employees of Imagicle direct or indirect processing subsidiaries located in the U.S.A, France, United Kingdom, United Arab Emirates, and Saudi Arabia
- providers/processors who process data on behalf of Imagicle

Processing by the parties as mentioned above is carried out, in addition to paper-based processing, with the help of electronic tools such as laptop PCs, desktop computers, servers, peccs, ordinary e-mail, SSDs, USB memory keys, memory cards, CD-ROMs and DVD-ROMs, hard drives (internal and external), cell phone memories, tablets, and cloud drives.

4 To whom are the data reported?

Imagicle may use third parties to provide the service. We do not rent or sell the information. Imagicle contracts with third-party service providers who can provide the same data protection and information security you can expect from Imagicle. The following is a list of the managers/sub-managers named concerning the processing:

IDENTIFICATION OF RESPONSIBLE PERSONS (OR SUB-RESPONSIBLE PERSONS).

Amazon Services SARL Web EMEA	<p>Manager's Address: Viale Monte Grappa 3/5, 24124, Milan (Italy)</p> <p>Purpose of Data Processing: AWS is entrusted, as a Cloud Service Provider, solely with ensuring the integrity and availability of the data stored on its servers. Therefore, AWS does not access personal data; the data is protected by additional security measures, such as encryption. AWS is used for hosting purpose and for artificial intelligence service like Text to Speech and Speech to Text capabilities.</p> <p>Categories of personal data: personal data related to the use of Imagicle Products and related Services</p> <p>Country where processing will take place: cloud services are managed through Amazon Web Services (AWS). Customers can request that their production hosting be in any country-specific AWS location proposed by Imagicle or in another AWS region of their choice</p> <p>Frequency of transfer: continuous/daily</p> <p>Guarantees that legitimize the transfer:</p> <ul style="list-style-type: none"> • United States: the transfer is made based on the presence of an adequacy decision (art 45 GDPR) adopted on 10.07.2023 by the European Commission (EU-U.S. DATA PRIVACY FRAMEWORK - "DPF"). The member organizations of the DPFA can be consulted at the following link: https://www.dataprivacyframework.gov/s/participant-search • Other countries with guarantee an adequate level of protection: transfer is permissible if the Commission has decided that the third country, a territory or specific sector(s) within the third country, or the international organization in question guarantee an adequate level of protection. In such a case, the transfer does not require specific authorization. The third country or organization's adequacy is recognized by the European Commission's decision (Article 45 of EU Regulation 2016/679) • Other countries: transfer is made based on the standard data protection clauses adopted by the European Commission, with provision for additional safeguards where deemed necessary, or based on Binding Corporate Rules (BCRs) (Art. 46 of EU Regulation 2016/679) <p>You can see all the information provided by AWS regarding data processing at the following link: https://aws.amazon.com/it/compliance/gdpr-center</p>
Salesforce Limited UK	<p>Manager's Address: Floor 26 Salesforce Tower, 110 Bishopsgate, EC2N4AY London. (United Kingdom)</p> <p>Purpose of Data Processing: this is a CRM software provider used for administration and business relationship management activities with customers/potential customers/end users only. Salesforce operators in the service and support phases of the product may, on an occasional basis and under the control of Imagicle personnel, access personal data</p>

Personal data categories: personal data processed to administer and manage the relationship with the customer/potential customer/end user

Country in which the processing activity will take place: worldwide

Frequency of transfer: continuous/daily

Guarantees that legitimize the transfer:

- United States: the transfer is made based on the presence of an adequacy decision (art 45 GDPR) adopted on 10.07.2023 by the European Commission (EU-U.S. DATA PRIVACY FRAMEWORK - "DPF"). The member organizations of the DPFA can be consulted at the following link:

<https://www.dataprivacyframework.gov/s/participant-search>

- Other countries with guarantee an adequate level of protection: transfer is permissible if the Commission has decided that the third country, a territory or specific sector(s) within the third country, or the international organization in question guarantee an adequate level of protection. In such a case, the transfer does not require specific authorization. The third country or organization's adequacy is recognized by the European Commission's decision (Article 45 of EU Regulation 2016/679)

- Other countries: Transfer is made based on the standard data protection clauses adopted by the European Commission, with provision for additional safeguards where deemed necessary, or based on Binding Corporate Rules (BCRs) (Art. 46 of EU Regulation 2016/679).

You can see all the information provided by Salesforce regarding data processing at the following link:

<https://www.salesforce.com/eu/company/privacy>

Manager's Address: 350 Bush Street, Level 13 San Francisco, California 94104 (USA)

Purpose of Data Processing: this cloud storage (archiving) and file-sharing service allows you to store, synchronize and share documents and other files via the Internet. Imagicle uses it for sharing and storing files and documents that may contain personal data of customers/potential customers/end Users related only to administration and business relationship management activities

Personal data categories: personal data processed to administer and manage the relationship with the customer/potential customer/end user

Country in which the processing activity will take place: worldwide

Frequency of transfer: continuous/daily

Guarantees that legitimize the transfer:

- United States: the transfer is made based on the presence of an adequacy decision (art 45 GDPR) adopted on 10.07.2023 by the European Commission (EU-U.S. DATA PRIVACY FRAMEWORK - "DPF"). The member organizations of the DPFA can be consulted at the following link:

<https://www.dataprivacyframework.gov/s/participant-search>

- Other countries with guarantee an adequate level of protection: transfer is permissible if the Commission has decided that the third country, a territory or specific sector(s) within the third country, or the international organization in question guarantee an adequate level of protection. In such a case, the transfer does not require specific authorization. The third country or organization's adequacy is recognized by the European Commission's decision (Article 45 of EU Regulation 2016/679)

Atlassian Inc

- Other countries: Transfer is made based on the standard data protection clauses adopted by the European Commission, with provision for additional safeguards where deemed necessary, or based on Binding Corporate Rules (BCRs) (Art. 46 of EU Regulation 2016/679)

You can see all the information provided by Atlassian regarding data processing at the following link:

<https://www.atlassian.com/it/legal/privacy-policy#what-this-policy-covers>

Manager's Address: Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Ireland

Purpose of the Data Processing: Microsoft 365 is a suite of enterprise collaboration software products. It is used by Imagicle for the management of various digital contents, among which texts, presentations, emails that may contain personal data of Customer and End User and data and Personal Data related to the use of Imagicle Products and in the fruition of related Services

Categories of personal data: Customer and End User personal data and data related to the use of Imagicle Products and in the fruition of related Services

Country where processing will take place: worldwide

Frequency of transfer: continuous/daily

Guarantees legitimizing the transfer

- EU
- United States: the transfer is made based on the presence of an adequacy decision (art 45 GDPR) adopted on 10.07.2023 by the European Commission (EU-U.S. DATA PRIVACY FRAMEWORK - "DPF"). The member organizations of the DPFA can be consulted at the following link:
<https://www.dataprivacyframework.gov/s/participant-search>
- Other countries do not ensure an adequate level of protection: the transfer is permitted if the Commission has decided that the third country, a territory or one or more specific sectors within the third country, or the international organization in question ensure an adequate level of protection. In that case, the transfer does not require specific authorizations. The adequacy of the third country or organization is recognised by decision of the European Commission (Art. 45 of EU Regulation 2016/679)
- Other countries: The transfer is made on the basis of the standard data protection clauses adopted by the European Commission, with provision for additional safeguards where deemed necessary, or on the basis of the Binding Corporate Rules (BCRs), (Art. 46 of EU Regulation 2016/679)

You can consult all the information provided by Microsoft on data processing at the following link: <https://privacy.microsoft.com/it-IT/>

**Microsoft
Ireland
Operations
Limited
Microsoft 365**

Manager's Address: One Park Place, Floor 5 Upper Hatch Street, Dublin (Ireland)

Purpose of Data Processing: this cloud storage (archiving) and file-sharing service allows you to store, synchronize and share documents and other files via the Internet. Imagicle uses it for sharing and storing files and documents that may contain personal data of Customers/Potential Customers/End Users related only to administration and business relationship management activities

**Dropbox
International
Unlimited
Company**

	<p>Personal data categories: personal data processed to administer and manage the relationship with the customer/potential customer/end user</p> <p>Country in which the processing activity will take place: worldwide</p> <p>Frequency of transfer: continuous/daily</p> <p>Guarantees that legitimize the transfer:</p> <ul style="list-style-type: none"> • United States: the transfer is made based on the presence of an adequacy decision (art 45 GDPR) adopted on 10.07.2023 by the European Commission (EU-U.S. DATA PRIVACY FRAMEWORK - "DPF"). The member organizations of the DPFA can be consulted at the following link: https://www.dataprivacyframework.gov/s/participant-search • Other countries with guarantee an adequate level of protection: transfer is permissible if the Commission has decided that the third country, a territory or specific sector(s) within the third country, or the international organization in question guarantee an adequate level of protection. In such a case, the transfer does not require specific authorization. The third country or organization's adequacy is recognized by the European Commission's decision (Article 45 of EU Regulation 2016/679) • Other countries: Transfer is made based on the standard data protection clauses adopted by the European Commission, with provision for additional safeguards where deemed necessary, or based on Binding Corporate Rules (BCRs) (Art. 46 of EU Regulation 2016/679). You can see all the information provided by Dropbox regarding data processing at the following link: https://www.dropbox.com/privacy
OpenAI	<p>Manager's Address: San Francisco, 3180 18th St, United States</p> <p>Purpose of Data Processing: Use of OpenAI artificial intelligence API for intent recognition and output generation</p> <p>Personal data categories: personal data related to the use of Imagicle Products and related Services</p> <p>Country where processing will take place: United States</p> <p>Frequency of transfer: continuous/daily</p> <p>Guarantees that legitimize the transfer: Appointment as Data Processor with adoption of Standard Contractual Clauses</p>
Pinecone	<p>Manager's Address: New York, 1375 Broadway, Floor 11, United States</p> <p>Purpose of Data Processing: Use of Pinecone Vector Database to build knowledgeable AI</p> <p>Personal data categories: personal data related to the use of Imagicle Products and related Services</p> <p>Country where processing will take place: United States, Europe</p> <p>Frequency of transfer: continuous/daily</p> <p>Guarantees that legitimize the transfer: Appointment as Data Processor with adoption of Standard Contractual Clauses</p>
Imagicle Ltd	<p>Manager's Address: Pixash Lane, Keynsham, Bristol</p> <p>Purposes of Data Processing: this direct subsidiary of Imagicle Spa works with it to administer and manage the relationship with the customer/potential customer/end user</p>

	<p>Personal data categories: personal data processed to administer and manage the relationship with the customer/potential customer/end user</p> <p>Country where processing activities will take place: United Kingdom</p> <p>Frequency of transfer: continuous/daily</p> <p>Guarantees that legitimize the transfer: Other countries with guarantee an adequate level of protection: transfer is permissible if the Commission has decided that the third country, a territory or specific sector(s) within the third country, or the international organization in question guarantee an adequate level of protection. In such a case, the transfer does not require specific authorization. The third country or organization's adequacy is recognized by the European Commission's decision (Article 45 of EU Regulation 2016/679). COMMISSION EXECUTIVE DECISION (EU) 2021/1773 of June 28, 2021, under Directive (EU) 2016/680 of the European Parliament and the Council on the adequate protection of personal data by the United Kingdom.</p>
Imagicle Sas	<p>Manager's Address: Parc des Barbanniers 5 - Promenade de la Bonnette - 92230 Genevilliers</p> <p>Purposes of the Data Processing: this is a direct subsidiary of Imagicle Spa that collaborates with it to administer and manage the relationship with the customer/potential customer/end user.</p> <p>Categories of personal data:</p> <ul style="list-style-type: none"> personal data processed to administer and manage the relationship with the customer/potential customer/end user personal data related to the use of Imagicle Products and related Services <p>Country in which processing activities will take place: France</p> <p>Frequency of transfer: continuous/daily</p> <p>Guarantees that legitimize the transfer: Not necessary, the transfer takes place within the territory of the European Union</p>
Imagicle Dmcc	<p>Manager's Address: Office 1307, JBC5, Cluster W, JLT - PO BOX 283982 United Arab Emirates</p> <p>P Purposes of the Data Processing: this direct subsidiary of Imagicle Spa works with it to administer and manage the relationship with the customer/potential customer/end user and for support activities</p> <p>Personal data categories: personal data processed to administer and manage the relationship with the customer/potential customer /end user</p> <p>Country in which processing will take place: United Arab Emirates</p> <p>Frequency of transfer: continuous/daily</p> <p>Guarantees that legitimize the transfer: Other countries: Transfer is made based on the standard data protection clauses adopted by the European Commission, with provision for additional safeguards where necessary</p>
Imagicle Saudi Communication Technology and Information	<p>Manager's Address: 7586 King Fahd Rd, 4119 Ar Rahmaniyah Dist, 12341 Riyadh, Kingdom of Saudi Arabia</p> <p>Purpose of Data Processing: this indirect subsidiary of Imagicle Spa works with it to administer and manage the relationship with the customer/potential customer/end user and for support activities</p> <p>Personal data categories: personal data processed to administer and manage the relationship with the customer/potential customer/end user.</p> <p>Country where processing will take place: Saudi Arabia</p> <p>Frequency of transfer: continuous/daily</p>

Guarantees that legitimize the transfer:

Other countries: Transfer is made based on the standard data protection clauses adopted by the European Commission, with provision for additional safeguards where necessary

Imagicle Inc

Manager's Address: 333, Las Olas Way - Fort Lauderdale FL33130 - United States

Purposes of the Data Processing: this direct subsidiary of Imagicle Spa, works with it to administer and manage the relationship with the customer/potential customer/end user and for support activities

Personal data categories: personal data processed to administer and manage the relationship with the customer/potential customer/end user.

Country in which processing activities will take place: United States of America

Frequency of transfer: continuous/daily

Guarantees that legitimize the transfer:

Appointment as Data Processor with adoption of Standard Contractual Clauses

5 Where does the treatment take place?

Data are processed at the operational headquarters of Imagicle and related companies (as described above).

For Cloud Products, the Customer chooses the location of data centers from those proposed by Imagicle or in other regions identified from those made available by AWS.

For reasons related to collaboration with third parties, the personal data provided may be transferred to a country other than the one where the User/Interested Person is located outside the European Economic Area (for more details, see the section " Identification of Responsible Persons (or Sub-Responsible Persons)", section 4.

6 What are the data retention and deletion policies?

As Data Processor/Sub Processor

- Personal data collected during support services, after three years from the service termination, all data will be delated
- Personal data collected during cloud services, after the termination of the End User License, the service will be disabled, and the data will be still accessible for end users for 30 days. In renewal, no action is taken on the data by Imagicle, and the service instance remains active. If the End User does not renew at the end of 30 days, the service will be terminated, and access to the data will be blocked: the End User Data will be kept in backup for up to 3 months (grace period). After 3 months, the End User Data will be deleted. During this period, the End User (or, for them, the reseller, where applicable) can request an export of the data to Imagicle with an e-mail addressed to gdpr@imagicle.com. The data stored in the database will be extracted in a format the Customer uses.
All related files will be exported to a network link for downloading by the Customer.

After the above time limits have expired, Imagicle will not retain any copies of the Personal Data unless required by law (and in such case, Imagicle will notify the Distributor/Dealer/Customer).

Regarding End-user data, Imagicle doesn't adopt any automatic retention policy. Data controller can adopt his internal policies and procedures.

For more details on retention and cancellation policy, contact Imagicle at the following e-mail address: gdpr@imagicle.com.

7 How can data subjects exercise their rights?

The Data Subject may exercise the rights provided by the GDPR (Articles 15-21), including:

- receive confirmation of the existence of Data and access to its content (access rights)
- update, modify and/or correct Data (right of rectification)
- request the deletion or limitation of the processing of Data processed in violation of the law, including Data whose retention is not necessary concerning the purposes for which the Data were collected or otherwise processed (right to be forgotten and right to limitation)
- oppose to the processing (right to object)
- propose complaints to the Supervisory Authority (Data Protection Authority www.garanteprivacy.it) in case of violation of personal data protection regulations
- receive an electronic copy of Data concerning him or her as a Data Subject when such Data has been rendered in the context of the contract, and request that such Data be transmitted to another data controller (right to data portability)

To exercise these rights, as stated in the disclosures, the Data Subject may contact Imagicle by sending a communication to gdpr@imagicle.com by visiting www.imagicle.com.

The Respondent should include his or her name, e-mail/postal address and/or phone number(s) to be sure that his or her request can be appropriately handled.

Requests received will be acknowledged by Imagicle, which will make the necessary verifications regarding the applicant's identity and, in particular, will verify that the applicant and data subject. Imagicle will invite the subject to fill out the Mod. Exercise of rights regarding the protection of personal data published by the **Italian Privacy Guarantor**. The form must be signed by the interested party and duly returned, accompanied by a copy of a valid identity document. Suppose the data subject is unable to complete and send the form above. In that case, the Data Controller shall acquire similar documentation for verifying the applicant's identity.

In the event of a successful outcome of such activities, it shall make the changes on the databases and files containing such data of the Interested Party and shall inform the same, without undue delay and in any case no later than within one month from the receipt of the request itself (this period may be extended by two months if necessary, taking into account the complexity and number of requests), by the same means in which the request for the exercise of rights was received, of the successful execution of the request.

Otherwise, in the event of a negative outcome of the verifications, it will notify the person concerned of the reason for the execution of the formulated request.

