

Product Specific Terms

Product	Actito Customer Engagement Platform
Product description	A Software as a Service (SaaS) solution accessible via a web interface allowing Customer's Users to perform a variety of marketing automation tasks such as, but not limited to, storing and retrieving Customer Data, launching campaigns, creating scenarios and analysing results.
Services provision	SaaS licence
Version	2026 Sep

OBLIGATIONS OF THE CUSTOMER.....	3
COMPLIANCE.....	3
LICENCE ADMINISTRATOR.....	3
USE OF THE SDK.....	3
CUSTOMER DATA UPON CONTRACT TERMINATION.....	4
ARTIFICIAL INTELLIGENCE	4
SECURITY AND SAFEGUARDS	4
PROFESSIONAL SERVICES.....	4
WORK ON INSTRUCTIONS AND VALIDATION BY THE CUSTOMER	4
TIME SHEETS	5
SERVICE LEVEL AGREEMENT	5
SUPPORT	5
SERVICE LEVELS	5
SERVICE CREDITS.....	6
DATA PROCESSING AGREEMENT	8
DATA PROCESSING ACTIVITIES	8
LIST OF SUB-PROCESSORS	10
SECURITY MEASURES.....	12

OBLIGATIONS OF THE CUSTOMER

COMPLIANCE

The Provider reserves the right to suspend the Services, in whole or in part, if the Customer does not comply with the relevant legislation (in particular with regard to consent to receive electronic communications) and/or if the Provider deems that the Customer's usage of the Product presents serious problems, namely in terms of deliverability (in particular in the event that the Provider notices blacklisting of IP addresses or domain names), without the use of this right being construed as a termination of the Contract. Deliverability problems are evaluated on the basis of observed or foreseeable information in terms of return rate to the sender ("Bounces"), number of complaints and/or unsubscribe requests linked to campaigns launched by the Customer. In the event of suspension of Services, the Customer will be notified at the same time as the suspension.

LICENCE ADMINISTRATOR

At least one person is designated by the Customer as the Product licence administrator. The name and the contact details of one licence administrator must be communicated to the Provider in writing within one (1) week of the signature of the Contract. The Product Licence administrator will subsequently provide access rights to the Customer's Users of its organization where appropriate and under the final control of such licence administrator. The Customer shall also maintain, at all times during any Service Term, at least one user within his organization who is authorized to administer the Customer's use of the Services.

USE OF THE SDK

The Customer shall integrate the SDK and ensure it is kept up to date in accordance with the Provider's instructions. The Provider shall not be held liable for the integration or the updating of the SDK within the Customer's application.

If the Contract terminates, whether due to expiry, rescission or termination, the licence granted to the Customer will end immediately and the Customer shall delete the SDK from its application and make all reasonable efforts to ensure that the application users

update the application so that it no longer contains the SDK. The Provider is not liable for any results of the use of the Services, including any damage to the application of the Customer caused by incorporating the SDK in the application of the Customer.

CUSTOMER DATA UPON CONTRACT TERMINATION

The Customer is responsible for exporting and erasing all its Customer Data from the Product before the termination date of the Contract. The Customer must interrupt any ongoing and future use of the Product (for example, interrupting the launch of campaigns, scenarios or processes, stop calling the Provider application programming interface (API)), at the latest on the fifteenth (15th) day preceding the termination date of the Contract, so as to allow the Provider to prepare the termination of the Services on the termination date. Should the Customer fail to do so, the Provider may suspend all accesses. The Provider will not retain any Customer Data for longer than thirty (30) days following the termination of the Contract, unless otherwise agreed in advance by the Parties in writing.

ARTIFICIAL INTELLIGENCE

SECURITY AND SAFEGUARDS

The latest and most detailed information on the security measures applicable to the AI Features is available as part of our Technical and Organisational Measures.

DESCRIPTION OF AI FEATURES

The latest and most detailed information on the AI Features included in the Product is available at our [Trust Center](#).

PROFESSIONAL SERVICES

WORK ON INSTRUCTIONS AND VALIDATION BY THE CUSTOMER

Professional Services are only provided on the Customer's instructions, and with the Customer's written approval. The Customer is responsible for validating in writing that the Professional Service delivered complies with the instructions within seven (7) days

of the provision of the Professional Service ordered. After this period, the Customer is deemed to have accepted it without reservation.

The Customer further acknowledges and agrees that the Provider may access the Customer's account for the purpose of delivering the Professional Services.

TIME SHEETS

The volume of Services provided by the Provider is tracked by an internal time sheet system recognized as valid by the Parties. The recording of each intervention is done in increments of every fifteen (15) minutes started.

The Customer acknowledges that the Provider's internal records offer sufficient evidence of the nature and extent of its use of the Services provided by the Provider and can be used as a base for invoicing.

SERVICE LEVEL AGREEMENT

SUPPORT

Channels

The primary Support channel is an email to support@actito.com.

Enhanced Support packages are available through the sales department to get access to the phone channel.

Hours

Standard Support is available during regular Office Hours (Monday to Friday, 09:00–18:00 UK & France local time), including public holidays.

Enhanced Support packages are available through our sales department to get access to extended hours:

- Monday to Friday: 08:00–20:00 (UK & France local time)
- Saturday & Sunday: 09:00–16:00 (UK & France local time)

SERVICE LEVELS

Service uptime

Uptime target: 99.5%.

First Response Time

First Response Time is measured within Office Hours.

Priority	Estimated response time
P1	2h
P2	4h
P3	8h
P4	Best effort

Mitigation time

Mitigation times in this table are objectives. Depending on the volume and priority of requests submitted to Support, response and resolution times may vary. Mitigation times are measured within Office Hours.

Priority	Mitigation time objective
P1	8h
P2	72h
P3	1080h
P4	Best effort

SERVICE CREDITS

Uptime	Credit
--------	--------

< 99,5% 10%

< 99% 25%

DATA PROCESSING AGREEMENT

DATA PROCESSING ACTIVITIES

Purpose and nature of processing	The Provider is required to process personal data entrusted to it by the Customer as part of the configuration, setting-up, triggering, management and analysis of the results of the Customer's marketing campaign through the Product. The Provider will only process personal data for the following purposes: (i) the performance of the Services in accordance with the Contract; and (ii) the performance of the reasonable instructions of the Customer to the extent that they comply with the terms of the Contract. Customer Data may be subject to the following processing: (i) storage and other processing necessary to provide, maintain and improve the Services provided to the Customer; and (ii) providing technical Support to the Customer.
Categories of personal data	The personal data processed by the Provider on behalf of the Customer is determined by the Customer, in particular when defining the type of data in the datamart. The Customer shall refrain, in the context of the use of the Product, from processing sensitive data, namely CVV number, IBAN number, as well as any personal data related to the unique identification of a person linked to the identity card, such as, but not limited to, the national identification number.
Duration of processing	During the provision of the Services, the duration of the data retention period is managed directly by the Customer through the Product data retention settings. The data retention period set by default is twenty-four (24) months and may be increased or decreased by the Customer.

At the end of the twenty-four (24) month period established by default or the period set by the Customer, the Customer will no longer be able to access the personal data. It is therefore the Customer's responsibility to adapt the duration according to the Customer's data retention policy.

Audit Trail of profiles	In order to allow the Customer to report, if necessary, proof of compliance with his obligation in terms of Personal Data, the Provider licence includes an Audit Trail feature which stores, for each profile in the database, a series of recordings, including a history of expressions of consent, subscriptions and deletions. The Audit Trail cannot be erased, either by the Provider or the Customer, as long as the licence is active.
-------------------------	---

LIST OF SUB-PROCESSORS

CM.com

Item	Description
About	https://www.cm.com/
Registered offices	CM Telecom France SAS 250 bis Boulevard Saint-Germain, 75007 Paris, France
Processing purpose	CPaaS (Communication Platform as a service) to send personalized messages (SMS) to mobile phones
Processing location	CM.com owns and operates its own datacentre located in the Netherlands
Security measures	• https://www.cm.com/trust-center/security/ • CM.com is certified ISO 27001, 27017, 27018, 9001, 14001, and 20000 • https://www.cm.com/cdn/web/en/file/iso27001-is-650045-001.pdf

OVH

Item	Description
About	https://www.ovh.com/
Registered offices	2 rue Kellermann, 59100 Roubaix, France
Contact	
Processing purpose	Domain Name System (DNS)
Processing location	OVH datacentres are located in Europe (3 datacentres in France, one in Germany and one in Poland)
Security measures	• https://www.ovhcloud.com/en/datacenters-ovhcloud/ • OVH is certified SOC 1 type II (SSAE 16 and ISAE 3402), SOC 2 type II and ISO 27001 • https://www.ovhcloud.com/en-gb/enterprise/certification-conformity/iso-27001-27017-27018/

Zendesk

Item	Description
About	https://www.zendesk.com/
Registered offices	Zendesk France 34 Avenue de l'Opéra, 75002 Paris, France
Contact	euprivacy@zendesk.com
Processing purpose	Online helpdesk ticketing service
Processing location	Zendesk datacenters are located in Europe (Frankfurt Germany)
Security measures	• https://www.zendesk.com/trust-center/ • Zendesk is certified ISO 27001, 27701, SOC 2

JIRA

Item	Description
About	https://www.atlassian.com/software/jira
Registered offices	Atlassian Pty Ltd, Level 6, 341 George St, Sydney NSW 2000, Australia
Contact	privacy@atlassian.com
Processing purpose	Issue escalation to level 2 support and to development teams
Processing location	Data residency configured in Europe (Frankfurt, Germany)
Security measures	• https://www.atlassian.com/trust/security/security-practices • https://www.atlassian.com/trust/data-protection • Atlassian maintains ISO/IEC 27001 certification and SOC 2 compliance reports. • Encryption in transit and at rest.

SECURITY MEASURES

For the latest version of our Technical and Organizational Measures, please visit our [Trust Center](#).