

Definitions

Except to the extent expressly provided otherwise, in the Agreement:

“Account” means an account enabling the Client to access and use the Hosted Services, including both the back-office account and the API account;

“Affiliate” means an entity that controls, is controlled by, or is under common control of, the relevant Party;

“Agreement” means the applicable Sales Order and Privacy Policy (including any amendments made to it from time to time) together with these Terms of Service including any Schedules, Exhibits or other Attachments hereof;

“Business Day” and **“Business Hours”** means any weekday other than a bank or public holiday in the United Kingdom; and the latter means the hours of 09:00 to 17:00 GMT (or BST during summertime) on a Business Day;

“Charges” means the following amounts:

The amounts specified in the applicable Sales Order for provision of Services; and Such amounts as may be agreed in writing by the parties from time to time.

“Charging Method” means the method of payment of Charges agreed between the Client and the Provider and specified as such on the applicable Sales Order. The Charging Method available for the Services are:

Pre-paid billing: wherein the Client shall pay upfront for an agreed amount of Hosted Services

usage; and

Subscription billing: The Client shall make periodic payments for the agreed usage of Hosted

Services following a predetermined billing cycle. Any usage exceeding the agreed commitment will be

charged based on actual usage. Unused capacity below the agreed commitment will not carry over, be

refunded, or adjusted in subsequent billing periods.**.

“Client” means the client listed in the applicable Sales Order, acting as the ‘Controller’ herein;

“Client Data” means all data, works and materials uploaded to or stored on the Platform by the Client; transmitted

by the Platform as and when requested by the Client; supplied by the Client to the Provider for

processing, uploading to, transmission by or storage on the Platform; or generated by the Platform as a

result of the use of the Hosted Services by the Client;

“Client Personal Data” means any Personal Data that is processed by the Provider on behalf of the Client in relation to the

Agreement;

“Client Systems” means the hardware and software systems of the Client that interact with, or may reasonably be expected to interact with, the Hosted Services;

“Confidential Information” means the information disclosed by either party, in writing, orally or otherwise, marked as confidential or which should have been reasonably understood to be confidential by the party in receipt of such disclosure and as provided under Clause 7 of this Agreement;

“Controller” has the same meaning given to it under the GDPR;

“Customization(s)” means a customization of the Hosted Services, whether made through the configuration or integration of software or otherwise;

“Data Protection Laws” means all applicable laws relating to the processing, privacy, and/or use of Personal Data including the *Data Protection, Privacy, and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019*, the *Data Protection Act 2018*, the *GDPR*, and the *Privacy and Electronic Communications (EC Directive) Regulations 2003*, including any laws that replace, extend, re-enact, consolidate, or amend any of the foregoing;

“Documentation” means any and all API documentation detailing the functions, classes, return types, arguments or any other information provided to effectively use the Hosted Services;

“EEA” means the European Economic Area including the UK;

“Effective Date” means the date when the Sales Order is countersigned by the last party to sign.

“Expenses” means the travel, accommodation and subsistence expenses that are reasonably necessary for, and incurred by the Provider exclusively in connection with, the performance of the Provider’s obligations under the Agreement;

“Force Majeure Event”

means any event beyond the reasonable control of a party (including a party’s Affiliates and/or subcontractors) including, but not limited to, the following: acts, events, omissions, or accidents beyond its reasonable control, including, without limitation, lock-outs, or other industrial disputes, failure of a utility service or transport or telecommunications network, act of God, malicious damage, compliance with any law or governmental order, rule, regulation, or direction, accident, breakdown of

plant or machinery, fire, flood, storm, epidemic or pandemic, or default of sub-contractors, to the

extent that such event has materially affected the ability of the party relying on the Force Majeure

Event to perform its obligations (other than the payment of moneys) in accordance with the terms of the

Agreement;

“GDPR” means the General Data Protection Regulation (Regulation (EU) 2016/679), including the version of the

same transposed into the UK law pursuant to the *European Union (Withdrawal) Act 2018*;

“Hosted Services” means online biometric verification services as specified in the Hosted Services Specification, which

will be made available by the Provider to the Client as a service via the internet in accordance with

the terms of the Agreement;

“Hosted Services Defect” means a defect, error or bug in the Platform having an adverse effect on the appearance, operation,

functionality or performance of the Hosted Services, but excluding any defect, error or bug caused by or

arising as a result of:

any act or omission of the Client or any person authorized by the Client to use the Platform or Hosted Services;
any use of the Platform or Hosted Services contrary to the Documentation, whether by the Client or by any person authorized by the Client;
a failure of the Client to perform or observe any of its obligations in the Agreement;
an incompatibility between the Platform or Hosted Services and any other system, network, application, program, hardware or software not specified as compatible in the Hosted Services Specification; and/or
Client's failure to implement corrections to the Hosted Services Defect.

“Hosted Services Specification” means the specification for the Platform and Hosted Services as set out in Schedule 1 and in the Documentation;

“Intellectual Property Rights” means all intellectual property rights wherever in the world, whether registrable or un-registrable, registered or unregistered, including any application or right of application for such rights (including, without limitation, copyright and related rights, database rights, confidential information, trade secrets, know how, business names, trade names, trademarks, service marks, passing off rights, unfair competition rights, patents, petty patents, utility models, semi-conductor topography rights and rights in designs);

“Personal Data” has the same meaning given to it under the GDPR;

“Platform” means the platform managed by the Provider and used by the Provider to provide the Hosted Services, including the application and database software for the Hosted Services, the system and server software used to provide the Hosted Services, and the computer hardware on which that application, database, system and server software is installed;

“Processor” has the same meaning given to it under the GDPR;

“Product(s)” means any or all of the Services as are specified in the Agreement and may include the onsite or offsite Face liveness, Facial recognition;

“Provider” means the party providing Hosted Services and listed as such in the applicable Sales Order, acting as a Processor herein;

“Sales Order” means, irrespective of its title, a cover document that sets out details of Services to be provided, duration of such Services, payment of Charges, and the applicable Charging Method, incorporating these Terms of Service signed by, and binding on, both parties;

“Schedule” means any schedule attached herein which form an integral part of these Terms of Service;

“Services” means any services that the Provider provides to the Client under the Agreement;

“Support Services” means support in relation to the use of, and the identification and resolution of errors in, the Hosted Services in accordance with Schedule 4 but shall not include the provision of training services;

“Supported Web Browser” means the browsers specified by the Provider for onsite or offsite verifications, and may include the current or latest release, from time to time, of Mozilla Firefox, Google Chrome or Apple Safari, or any other web browser that the Provider notifies to the Client in writing;

“Term” has the meaning given to it in the applicable Sales Order;

“Termination for Cause” means, subject to Clause 13, where the Agreement is terminated if either party engages in any of the following: (i) acts of misconduct involving dishonesty or breach of trust; (ii) willful conduct in bad faith that significantly harms the other party, such as misappropriation of Confidential Information, fraud, or embezzlement; or (iii) a material breach of the Agreement.;

“Third-Party Services” means any or all Products or Services ancillary to the Hosted Service(s) and may include any Products or Services provided by the Provider’s sub-processors;

“UK” means the United Kingdom;

“Update” means a hotfix, patch or minor version update to any Platform software;

“Upgrade” means a major version upgrade of any Platform software;

“US\$” means the currency/Dollar of United States of America; and

“€” means the Euro currency used in majority countries of the European Union.

“Verifier Registrar” means the Provider’s role as an intermediary infrastructure provider facilitating identity and credential verification between Clients and third-party providers, without issuing credentials or making final verification decisions.

“Verification Data” means any identity data, credential data, or output generated through the Hosted Services.

“End User” means any individual whose identity or data is processed through the Hosted Services.

Hosted Services

To access Hosted Services, the Client must submit a Sales Order. The Provider will draft the Sales

Order to outline the details of the purchased services, applicable fees, chosen Charging Method, and any specific conditions. The agreement will become binding once both parties sign it.

Unless otherwise stated in Clause 2.4, Clause 6.3, and Clause 13, the Term will automatically renew under the current Terms of Service or any amendments applicable at the time, unless one party notifies the other in writing of their intention not to renew.

The Provider grants the Client a limited, non-exclusive, non-transferable, non-sublicensable, and revocable right to access and utilize the Hosted Services through a Supported Web Browser, in accordance with the Documentation, for the duration of the Agreement.

The Client is prohibited from sublicensing access, allowing unauthorized users to access Hosted Services, redistributing any content from the Hosted Services, or modifying the Platform in any way.

The Client must ensure that unauthorized users do not gain access and must maintain reasonable security measures.

Schedule 2 governs service availability. The Provider is not responsible for any data sent or received through the Hosted Services. The Client is responsible for using the Hosted Services in a manner consistent with applicable laws, regulations, and the Provider's policies.

All Intellectual Property Rights related to the Hosted Services and Documentation remain the sole

property of the Provider. The Client has no ownership or proprietary rights in the Software,

Documentation, or Services beyond the limited rights granted herein. The Client shall not modify,

decompile, disassemble, reverse engineer, sublicense, sell, or lease the Provider's Intellectual Property.

The Hosted Services must not be used in any way that causes disruption, harm, or degradation of

service. The Client has no right to access any software code (including source,

intermediate, or
object code) during or after the Term.

Permitted Use of Hosted Services

The Client shall use the Hosted Services solely for lawful, legitimate, and disclosed identity verification purposes

The Client shall not:

- (a) conduct surveillance, tracking, or monitoring of individuals;
- (b) perform profiling or automated decision-making without a valid legal basis;
- (c) use verification outputs for discriminatory or unlawful purposes;
- (d) initiate verification without obtaining valid end user consent;
- (e) use verification data beyond its disclosed purpose.

All rights not explicitly granted to the Client are reserved by the Provider.

Any Customizations made for the Client remain the Provider's exclusive property.

Any modification, extension, or alteration made by the Client is automatically assigned to the Provider.

The Client

must not use, permit, or enable any third party to utilize the Hosted Services to create competing products or services.

Verifier Registrar Role and Scope

The Provider operates as a Verifier Registrar and provides infrastructure enabling Clients to access identity verification services.

The Provider does not:

- (a) issue identity credentials;
- (b) guarantee the authenticity or validity of credentials;
- (c) make decisions regarding acceptance or rejection of verification results.

All verification decisions and reliance on outputs remain the sole responsibility of the Client.

Client Obligations

Unless otherwise agreed in writing, the Client must provide the Provider with necessary cooperation, support, information, and documentation required to comply with applicable laws, including Data Protection Laws.

The Client is responsible for ensuring that its hardware and software systems are compatible with the Hosted Services and must comply with the requirements of Schedule 1. Any changes must be agreed upon in writing.

Without express written permission, the Client may not resell, white-label, or rebrand the Hosted

Services. The Client must:

Notify third parties regarding data use and disclosure in compliance with applicable laws.

Obtain the necessary permissions for the Provider to process third-party data.

Refrain from using the Hosted Services for illicit, misleading, or malicious activities, including

transmitting harmful software.

Monitor and regulate its personnel using the Hosted Services.

Comply with all applicable laws when using Hosted Services.

Client Personal Data

The Client warrants that its use of Personal Data complies with all applicable laws and does not infringe any third-party rights.

The Provider may use the Client's name, trade name, trademark, and logo for promotional purposes, including online platforms and marketing campaigns. Any use by the Provider benefits the Client, who retains ownership of its brand assets.

CREDENTIAL USE RESTRICTIONS

Use of Verification Data

The Client shall

(a) use verification data solely for the specific purpose disclosed to the End User;

(b) not retain data longer than necessary;

- (c) not create independent identity databases without lawful basis;
- (d) not combine verification data with other datasets for unrelated purposes;
- (e) comply with all applicable data protection laws in downstream use.

Integrations with Third-Party Services

The Client hereby grants express permission for the integration of the Hosted Services with services rendered by Third-Party Services, with the intent to provide a comprehensive set of Hosted Services.

The Provider reserves the unencumbered right, at its sole discretion, to revoke, curtail, or impose limitations upon any integration involving Third-Party Services.

The Client expressly recognizes and concurs that the synthesis of such Third-Party Services might necessitate the transference of Client Data from the Hosted Services to the corresponding Third-Party Services.

Third-Party Services: Verifications

The Provider has integrated a few services provided by third parties. By using our services, you acknowledge and agree to the following terms regarding third-party service providers.

Scope of Third-Party Services:

The Provider facilitates access to these services powered by third-party, but the Provider does not own, control, or modify these services.

These services involve extracting, processing, and verifying user-submitted data (e.g., identity documents, biometric information) for identity authentication and fraud prevention.

While the Provider aims to provide seamless access, the Provider does not guarantee the accuracy, reliability, or availability of these services at all times.

Data Processing, Storage & Privacy

All data associated with the Services provided to the Client related to the third party Services is

transmitted directly to third-party systems designated for data processing or storage. The Service

Provider does not retain, store, or archive such data on its own servers or infrastructure. The

responsibility for data storage, security, and compliance rests solely with the third-party provider

receiving the data.

User data provided for verification purposes will be processed by the third-party in accordance

with their privacy policies, security protocols, and applicable data protection laws (e.g., GDPR, CCPA).

Data may be stored temporarily or for an extended period for legal compliance requirements.

The Provider do not assume liability for third party's handling, storage, or security of user data

beyond what is mutually agreed between the third-party and the Provider.

In the event that the Client requests access to any stored data, the Service Provider shall

retrieve the specific data from the third-party system and make it available to the Client. The

retrieved data shall be stored temporarily on the Service Provider's server solely for the purpose

of fulfilling the Client's request and shall be permanently deleted from the Service Provider's

systems immediately after the request has been fulfilled.

User Consent & Responsibilities:

The Client shall obtain explicit, informed, and verifiable consent from End

Users prior to:

collecting or processing identity or biometric data;

initiating any verification process;

sharing data with the Provider or third-party services

The Client shall clearly disclose:

By using our services, users explicitly consent to their data being processed by third-party for authentication and fraud prevention purposes.

Users must provide accurate and valid information to avoid verification failures.

The Provider does not guarantee verification success—approval or rejection depends on

third-party's assessment of the provided data.

Users are responsible for ensuring their data complies with legal and regulatory requirements

applicable in their jurisdiction.

Service Limitation & Availability

The services may experience downtime due to maintenance, system updates, or technical failures

by the third party.

The Provider reserves the right to modify, suspend, or discontinue these services at any time,

especially if third-party changes their terms, pricing, or service availability.

Service results may vary due to factors such as document quality, network issues, or regulatory

restrictions.

Compliance & Legal Obligation

Service Provider and third-party comply with GDPR, CCPA, and other relevant regulations, but users

shall ensure that their use of verification services aligns with their local laws.

If required by law, user data may be disclosed to authorities, regulatory bodies, or law

enforcement agencies.

Users acknowledge that third-party may transfer data across jurisdictions as permitted under

applicable data protection laws.

Liability & Indemnification

Service Provider is not liable for errors, inaccuracies, delays, or system failures caused by

third party's services.

The Provider does not warrant that third-party services will be error-free, uninterrupted, or meet specific user needs.

Users agree to indemnify and hold harmless Facia.ai from any claims, damages, or liabilities arising from third party's service failures, incorrect verifications, or data processing errors.

Termination & Service Charges

Facia.ai reserves the right to terminate or alter access to services based on operational needs, legal requirements, or changes in our agreement with the particular third party. In case of termination, users may no longer be able to access verification services, and any pending verifications may be cancelled without liability on our part. Continued use of these services after any modifications constitutes acceptance of the updated terms.

Third-Party Services: Storage

The Hosted Services may integrate with third-party platforms, including digital wallet providers.

Use of such platforms is subject to their respective terms and policies. The Provider shall not be responsible for:

- (a) platform availability or decisions;
- (b) acceptance or rejection of integrations;
- (c) actions taken by such platforms.

Service Level Guarantees & Penalties

Third-Party Dependency

Facia.ai has integrated a third-party service provider for hosting and server infrastructure. As a result, all uptime, downtime, accessibility issues, errors, and delays related to its servers are beyond Facia. Ai's control and liability. Users acknowledge that Facia.ai does not guarantee uninterrupted service due to this dependency.

No Liability for Downtime

Facia.ai shall not be held responsible for any loss, business disruption, or other consequences resulting from downtime, server inaccessibility, or performance issues caused by third-party.

No Refund Policy for Downtime

In case of extended or repeated downtimes, no refunds shall be issued. Facia.ai will, however, actively coordinate with it to resolve any service disruptions promptly.

Server Redundancy & Backup Strategy

As a precautionary measure, we maintain servers in multiple locations and implement a robust fallback mechanism with a comprehensive backup strategy. In the event of an issue affecting a primary server, the fallback servers automatically assume the primary role, ensuring seamless functionality

and
uninterrupted operations.

Data Retention & Deletion Policy

Data Retention Period

Facia.ai maintains a six (6) months data retention policy after termination of the Agreement.

Client/user data shall be stored securely during this period, subject to applicable regulations.

Use of Data for AI Model Optimization

By using Facia.ai's services, the users explicitly consent to Facia.ai utilizing their data to optimize, improve, and train AI models, ensuring enhanced accuracy, efficiency and o its AI-driven services, Any data used for such purposes shall be processed in compliance with applicable data protection regulations and anonymizations standards, where required.

Explicit Data Deletion Requests

Users may request deletion of their data by sending an email to:

tech@facia.ai

support@facia.ai

Upon receiving a valid deletion request, Facia.ai shall process it in compliance with its internal security protocols and regulatory obligations.

No Recovery Post-Deletion

Once data is deleted as per a user's request, it cannot be recovered. Users must ensure they have backup copies before submitting deletion requests.

Third-Party Liability Disclaimer

No Responsibility for Third-Party Failures

The Provider undertakes reasonable diligence in selecting third-party service providers. However, the Client acknowledges that such providers operate independently, and the Provider shall not be liable for their acts or omissions except where required by applicable law.

Service interruptions due to third party's downtime.
Data breaches arising from third party's security failures.
Legal or contractual disputes involving third party .

Client Acknowledgment

By using Facia.ai's services, clients acknowledge and accept that a third party operates independently,
and Facia.ai does not assume liability for their actions or inactions.

Ai & Algorithm Accountability & Bias Mitigation

Performance Metrics & Limitations

Facia.ai's AI-driven solutions, including biometric verification, utilize machine learning algorithms.

While our system has undergone rigorous third-party evaluations, users acknowledge that:

AI-based verification is not 100% error-free and can be influenced by external factors.

Facia.ai guarantees reasonable commercial viability and accuracy, but no absolute certainty.

Third-Party Certification

Facia.ai has achieved 100% accuracy certification from iBeta, a third-party evaluation body in the US.

This certification reflects the system's high performance and reliability in biometric verification.

AI Errors & No Liability

AI models may generate false positives or false negatives due to data quality, environmental conditions, or inherent biases. Facia.ai shall not be liable for any incorrect verification results or associated consequences.

Intellectual Property (IP) & Branding

Ownership of Custom Solutions

Any intellectual property (IP) resulting from customizations requested by a client shall remain the property of Facia.ai, even if a license fee is paid. Clients shall not claim ownership over any AI models, enhancements, or proprietary methodologies.

Use of Client Logos & Branding

Facia.ai reserves the right to feature client logos, testimonials, and partnerships on its website, marketing materials, and social media platforms. Clients may request exclusion from promotional use by contacting support@facia.ai.

Intellectual Property (IP) & Branding

Ownership of Custom Solutions

Any intellectual property (IP) resulting from customizations requested by a client shall remain the property of Facia.ai, even if a license fee is paid. Clients shall not claim ownership over any AI models, enhancements, or proprietary methodologies.

Use of Client Logos & Branding

Facia.ai reserves the right to feature client logos, testimonials, and partnerships on its website, marketing materials, and social media platforms. Clients may request exclusion from promotional use by contacting support@facia.ai.

Data Collection from Public Sources

Facia may collect, process, and use data from publicly available sources, including but not limited to publicly accessible websites, social media platforms, government records, and other open data repositories. This data may be used to improve our services, enhance our algorithms, and ensure the accuracy and reliability of our technology.

By using our services, you acknowledge and agree that Facia may incorporate publicly available data into its systems, provided such collection and use comply with applicable laws and regulations. If you believe that your data has been used in a manner inconsistent with your rights, you may contact us at support@facia.ai OR legal@facia.ai to request review or removal where applicable.

Payments

The Client must pay all applicable fees and charges as specified in the Sales Order. Payments are due within ten (10) days of invoice issuance.

Late payments may result in:

Interest accruing at an annual rate of 9% above the Bank of England's base rate.

Additional compensation as per the Late Payment of Commercial Debts (Interest) Act 1998.

Temporary suspension of services until outstanding amounts, including interest, are paid in full.

Prepaid & Unused Services

Facia.ai offers prepaid service plans where users purchase verification checks or API access in advance. Unused verification checks will neither be rolled over to the next term nor refunded.

All service plans are subject to automatic renewal at the end of each term. Users who do not wish to renew must provide written notice at least 1 month prior to the renewal date.

Refund Policy

Facia.ai does not offer refunds for prepaid but unused services. Clients are encouraged to use their purchased quotas within the designated period.

Pricing Adjustments

Facia.ai reserves the right to modify pricing, payment terms, or service plans at its discretion.

Clients will be informed at least 30 days in advance of any changes affecting ongoing service agreements.

Acceptance of Terms

By using Facia.ai's services, users explicitly acknowledge and agree to the above Terms &

Conditions, including third-party service dependencies, AI performance limitations, liability

exclusions, and data retention policies.

For any inquiries or clarifications, please contact:

support@facia.ai

legal@facia.ai

Unused Verification Checks

Any unused verification checks remaining at the end of a billing cycle or contractual term shall

not be carried over to any subsequent term.

The Client acknowledges that unused checks will expire upon the completion of the applicable term,

and no refunds, rollovers, or credits shall be issued for any unused portion. The Client is

responsible for utilizing the allocated verification checks within the designated term.

Confidentiality

Pursuant to the negotiation and execution of this Agreement, both Parties acknowledge that they

might gain access to or be exposed to the Confidential Information of the other Party. Such

Confidential Information may encompass, but is not limited to, proprietary trade

secrets,
computational codes and programs, algorithms, operational features, non-public inventions, technical methodologies, procedural blueprints, software designs and structures, product and service specifics, as well as data about vendors, employees, consultants, clients, potential clients, and various technical, commercial, pricing, fiscal, and marketing strategies. It might also include any other data that, under reasonable circumstances, the receiving Party should recognize as confidential. To this end, both parties covenant to:

- Safeguard the Confidential Information of the other Party with the equivalent level of precaution it employs for its own similarly confidential data;
- Abstain from revealing the other Party's Confidential Information to any third-party without the prior written approval from the said party, ensuring that any such disclosure is contingent upon written confidentiality stipulations sanctioned by the Party to whom the Confidential Information pertains;
- Continually act with utmost good faith concerning the Confidential Information of the other Party;
- and
- Limit the use of the other Party's Confidential Information strictly to the intended purposes for which it was shared.

Notwithstanding the provisions set forth in Clause 8.1, a party's Confidential Information may be divulged by the recipient to its directors, personnel, legal counsel, insurers, representatives, and subcontractors who necessitate access to the aforesaid Confidential Information in furtherance of their duties related to the Agreement and who are contractually obligated, whether through a formal written instrument or an executed non-disclosure agreement, to maintain the

secrecy of the shared
Confidential Information.

This Clause 10 does not impose duties regarding a party's Confidential Information if said

Confidential Information:

is accessible to a party from a non-confidential source not currently, or previously, bound by a

non-disclosure commitment concerning the Confidential Information.

contemporaneous with or subsequent to the disclosure, is legitimately procured from sources in the

public domain (excluding instances resulting from a disclosure by the receiving party or its

representatives); or

is autonomously obtained or formulated by a party without contravening its responsibilities under

this Agreement or any applicable law or is secured by either party from a third entity where the

other party has no grounds to suspect a breach of a duty of confidentiality.

Limitations set forth in this Clause 10 are non-operative if any Confidential Information must be

disclosed due to legislative or regulatory mandates, any judicial or governmental directive or

request, or any stock listing prerequisites for either party on a recognized stock exchange.

Upon the termination of the Agreement, each party shall forthwith discontinue utilization of the

other party's Confidential Information; within five (5) Business Days post receiving a written

request for termination from the other party, the respective party must obliterate or revert (at the

discretion of the other party) all media, tangible or otherwise, containing the Confidential

Information of the other party and must expunge said Confidential Information.

The stipulations of this Clause 10 remain operative for a duration of three (3) years post the

termination of the Agreement.

The parties are precluded from executing public disclosures relating to the Agreement or its

contents (inclusive of statements in press releases, public proclamations, and marketing materials) devoid of prior written consent from the Provider, such consent not to be unreasonably withheld or postponed.

Data Protection

In compliance with the Agreement, both parties shall comply with the provisions of the Data

Protection Laws regarding the processing of Personal Data. The Provider shall solely handle the

Client Data in accordance with the documented instructions of the Client, as outlined in the

Agreement or any additional written agreement between the parties.

Notwithstanding anything to the contrary contained herein, the Provider may, if required by

applicable law or a lawfully invested authority, disclose the Client Data in such manner as

stipulated by such requirement. In such instances, save to the extent prevented by law, the

Provider shall endeavor to give the Client prompt notice of said disclosure.

As of the Effective Date, the Client authorizes the Provider to engage third parties for the

processing of Client Data. The Provider must inform the Client at least fourteen (14) days in

advance of any proposed changes in the use of a third-party processor. If the Client disagrees with

the planned changes before they are made, the Client has the right to terminate the Agreement by

providing written notice to the Provider within seven (7) days of the Provider's notification of the

upcoming changes. The Provider must ensure that all third-party processors comply with legal

obligations similar to those imposed on the Provider..

Both the Provider and Client must establish appropriate technical and organizational protocols to

ensure a satisfactory level of protection for the Client Data, including measures outlined in

Schedule 5.

The Provider must ensure that individuals authorized to handle the Personal Data either commit to maintaining confidentiality or are subject to an applicable legal confidentiality requirement.

The Client confirms and guarantees to the Provider its legal right to disclose all Personal Data in connection with the Agreement. Additionally, only Personal Data of individuals within specified categories in the Sales Order will be provided by the Client to the Provider. The Provider is limited to processing Client Data for purposes specified in Schedule 5.

For the duration of the Term and any additional periods required by relevant laws, the Provider shall exclusively handle the Client Data in accordance with the provisions of this Clause 8.

The Client acknowledges that Client Data may be transferred beyond the boundaries of the European Economic Area (EEA) in accordance with the execution of this Agreement and Standard Contractual Clauses (SSCs). The Client is responsible for obtaining the necessary consents for such transfers.

Additionally, if required by Data Protection Laws, the Provider may request a separate data processing agreement to be negotiated with the Client.

The Provider will assist the Client in upholding obligations related to the security of processing Personal Data, notifying breaches, conducting impact assessments, seeking prior consultation for high-risk processing, and facilitating the exercise of data subject rights under the Data Protection Laws.

Should any changes or upcoming updates to the Data Protection Laws result in non-compliance regarding the processing of Personal Data as set out in the Agreement, both parties will promptly work together to agree on the required modifications to the Agreement to address such non-compliance.

Warranties

The Provider hereby covenants to the Client that:

it shall comply with all applicable statutory and regulatory requirements relevant to the exercise

of its rights and the fulfilment of its obligations under this Agreement;

The Platform shall incorporate security measures in line with current industry practices; and

The Hosted Services, when used in accordance with this Agreement by the Client, must comply with

all relevant laws under English jurisdiction and must not violate the Intellectual Property Rights

of any person or entity, regardless of jurisdiction or legal framework in force.

The Client hereby recognizes and acknowledges that:

Using the Hosted Services is exclusively at the Client's discretion and risk. The Provider does not

guarantee that the service is fit for any purpose whatsoever or will meet all of the Client's needs

or that the operation of the Hosted Services will always be smooth and error-free.

the Hosted Services and related elements are tendered "in their current state" and "subject to

availability", inclusive of all defects, and the Provider categorically waives all express, implied,

or statutory warranties and conditions, except those that cannot be excluded under Applicable Law,

pertaining to the Hosted Services and affiliated elements, including, but not limited to,

warranties of merchantability, satisfactory quality, specific utility, precision, undisturbed

enjoyment, and non-infringement of third-party rights. Neither verbal nor written instructions from

the Provider or its subsidiaries shall be deemed to create any warranty, whether implied or

express.

software of intricate nature is invariably not devoid of imperfections, discrepancies, glitches, or

potential security breaches; and, contingent upon other stipulations of the Agreement, the Provider

abstains from providing any warranties or assurances that the Hosted Services shall

remain

impervious to such flaws or that such flaws shall be rectified expeditiously.

The Hosted Services have been customized to align only with the software and systems specified as

compatible in the Hosted Services Specification. The Provider does not warrant or guarantee that the

Hosted Services will be compatible with any other software or systems.

The Provider does not warrant absolute precision in outcomes or strict adherence to a 5-second

verification timeframe; slight deviations may occur infrequently due to factors such as spikes in

website traffic or the quality of verification documentation.

Any financial obligations in the form of Charges, regardless of whether the Hosted Services are

used or not, once incurred, are irrevocably due and payable and binding on the Client and cannot be

refunded or varied, except as specified in a validly executed Sales Order..

The Client confirms that it has had the opportunity to seek advice from its own legal counsel

regarding this Agreement, has thoroughly reviewed this Agreement, understands its terms, and is

signing this Agreement voluntarily, without any pressure or undue influence from the Provider or any

other party.

It is understood and accepted by the Client that when entrusting the Provider with Personal Data of

its consumers or end-users for processing, the Client is responsible for obtaining consent from its

consumers or end-users and ensuring compliance with Data Protection Laws before transferring the

Personal Data to the Processor. After such transfer, the Client must maintain and enforce a privacy

policy in accordance with Data Protection Laws..

This Agreement constitutes the entire agreement between the parties with respect to its subject

matter and supersedes all prior and contemporaneous agreements and understandings, whether written

or oral. The Parties shall have no other obligations or liability save as set out herein

or arising
from the express terms hereof. To the maximum extent permitted by the applicable law, all terms implied by statute or common law are excluded.

Each Party guarantee to the other that to the best of its knowledge and belief:
the individual signing this Agreement on their behalf possesses the requisite authority to do
so;

the execution of this Agreement does not contravene any prior agreements to which they are party.

Except for the warranties stated above, both parties hereby disclaim all express or implied representations and warranties related to this Agreement to the fullest extent allowed by current applicable law.

The Provider makes no guarantees or promises regarding the effectiveness, results, or advantages of the services, or any information included in or supplied under this Agreement, except as explicitly stated herein.

No agent or representative of the Provider has the authority to modify, expand, or further explain this limitation or the disclaimer of representations, warranties, and related terms set forth in this Agreement.

In the event of a breach of any representations or warranties set forth in this Agreement (excluding fraudulent misrepresentation), the party in breach shall be obligated to promptly take all commercially reasonable steps to remedy such breach.

Client Indemnities

In the event of breach by the of this Agreement, the Client agrees to indemnify and hold harmless the Provider from any liabilities, damages, losses, costs, and expenses, including attorney's fees and all legal costs. This indemnification covers loss and damages suffered by the

Provider directly
or indirectly as a result of the Client's breach. Furthermore, the Client agrees to:
extend to the Provider any and all cooperation and assistance as may reasonably be
solicited by the
Provider;
grant the Provider full and exclusive control over handling, resolving, and settling all
disputes,
legal matters, negotiations, and agreements with third parties; and
abstain from accepting liability or arriving at any settlements concerning disputes or legal
confrontations with third parties without securing the prior written consent of the
Provider. It is
imperative to note that any commitment on the part of the Provider to compensate
the Client is
rendered null and void unless the Client strictly adheres to the stipulations of this
Clause.

Limitations and Exclusions of Liability

Subject to this Clause 14, the Provider's liability to the Client shall be limited to
obligations:

Relating to this Agreement, including obligations under any indemnification
provisions;

In connection with the Client's use of the Hosted Services and Documentation;

In respect of any claims of tort, whether negligent or otherwise, arising from this
Agreement.

The terms of this Agreement shall not limit or exclude:

Any liabilities for death or bodily harm resulting from negligence;

Any liabilities for deceit or fraudulent misrepresentation;

Any obligations that cannot be waived under relevant statutory provisions;

Any obligations that are non-disclaimable under the governing law;

Any obligations specified in Clauses 1, except Clause 1.6.

Notwithstanding Clause 13.1, the Provider shall not be liable, whether in contract,
tort (including
negligence or breaches of statutory duties), misrepresentations, restitution claims,
or any other
claims arising from this Agreement, for:

Loss of anticipated revenue, business interruptions, projected savings, business opportunities,
goodwill depletion, data loss, or similar losses (whether direct or consequential);
Any direct, indirect, or consequential damages, costs, fees, or financial burdens;
total financial liability of the Provider for any single incident or a series of related incidents,
whether in contract, tort (including negligence or statutory breaches),
misrepresentations,
restitution claims, or other claims arising from this Agreement, shall not exceed the lesser
of:

USD 5,000; or

The total amount paid or due to be paid by the Client to the Provider within the three months
preceding the incident(s).

The Client shall not be liable to the Provider for losses resulting from a Force Majeure
Event.

To the maximum extent permitted by law, and notwithstanding anything to the contrary contained
herein, the Provider shall not be liable to the Client for any indirect, consequential, or special
losses or damages arising out of or in connection with this agreement, including but not limited to
loss of profits, revenue, business, or goodwill.

Force Majeure Event

In the event that a Force Majeure Event causes a delay or inability to fulfil any contractual
obligation under the Agreement by either party (excluding any fiduciary duties), such obligation
shall be temporarily suspended for the duration of the Force Majeure Event.

Should a party experience a Force Majeure Event that causes or is expected to cause a failure or
delay in meeting its contractual obligations under the Agreement, the party must promptly inform the
other party and provide an estimate of the expected duration of the delay.

Each Party who is unable to comply with the terms of the Agreement due to a Force Majeure Event, shall take all reasonable steps to mitigate the impact of the Force Majeure Event. In no event shall a Force Majeure Event release the Client from the responsibility to pay the Charges as specified in this agreement.

Term and Termination

Subject to the terms set forth in this Agreement, this Agreement shall come into force on the

Effective Date and shall remain in force for the duration of the Term.

Each Party may terminate this Agreement subject to written notice given by at least thirty (30)

days prior to the intended termination date.

A Party may terminate this Agreement for breach ("Termination for Cause") subject to giving written

notice to the defaulting party within seven (7) days following first becoming aware of occurrence of

such breach demanding rectification of the breach within a time frame of no less than fourteen (14)

days from the date of notification of breach. If the defaulting party remains non-compliant without

rectifying the identified breach within the designated fourteen (14) days period, the Agreement

shall terminate upon the expiry of such fourteen (14) days period.

SUSPENSION / RISK CONTROL

Suspension for Risk and Compliance

The Provider may suspend or restrict access to the Hosted Services immediately where it

reasonably determines that:

- (a) misuse or fraud is suspected;
- (b) the Client is in breach of this Agreement;
- (c) continued use poses legal, regulatory, or security risk;
- (d) required by law or third-party platform obligations.

Governing Law & Jurisdiction

This Agreement is governed by the laws of England and Wales. Any disputes shall be resolved exclusively by the courts of London, England.

Interpretation

Clause, Schedule and paragraph headings shall not affect the interpretation of this agreement.

A person includes a natural person, corporate or unincorporated body (whether or not having separate legal personality),

The Schedules form part of this agreement and shall have effect as if set out in full in the body of this agreement. Any reference to this agreement includes the Schedules.

A reference to a company includes any company, corporation or other body corporate, wherever and however incorporated or established.

Unless the context otherwise requires, words in the singular include the plural and, in the plural, include the singular.

This agreement shall be binding on, and enure to the benefit of, the parties to this agreement and their respective personal representatives, successors and permitted assigns, and references to any party includes that party's personal representatives, successors and permitted assigns.

A reference to writing or written excludes fax and email.

Any reference to an English legal term for any action, remedy, method of judicial proceeding, legal document, legal status, court, official or any legal concept or thing shall, in respect of any jurisdiction other than England, be deemed to include a reference to that which most nearly approximates to the English legal term in that jurisdiction.

A reference to this agreement or to any other agreement or document is a reference to this

agreement or such other agreement or document, in each case as varied from time to time.

References in the Agreement to “calendar months” are to the twelve (12) named periods (January, February and so on) into which a year is divided.

ASSIGNMENT AND CHANGE OF CONTROL

The Client shall not assign, transfer, charge, sub-contract, or novate this Agreement or any of its

rights or obligations under it without the Provider’s prior written consent.

Provider Rights: The Provider may at any time assign, transfer, novate, sub-contract, or otherwise

deal with all or any of its rights or obligations under this Agreement, including without limitation

in connection with a change of control, corporate restructuring, acquisition, or merger.

Brand Name and Control Changes: For any change that does not alter the Provider’s legal entity

(i.e., its company registration number remains the same), including changes to brand name, trading

name, ownership, or shareholders, the Provider has no obligation to provide any notice whatsoever,

whether prior or subsequent. The Client expressly waives any right to receive such notice.

Legal Entity Changes: If the Provider assigns or novates this Agreement to a different legal entity

(resulting in a different company registration number), the Provider shall provide the Client with

written notice within ten (10) Business Days after the effective date of such change.

No prior

consent is required. Any such assignment or novation shall be conditional upon the assignee

executing a written instrument assuming all obligations of the Provider under this Agreement,

including without limitation the data protection obligations set forth in Clause 12 (Data

Protection). The Client’s sole remedy for any objection to such change shall be to terminate this

Agreement without penalty by providing written notice within thirty (30) days of receiving the notice under this sub-clause 19.4, such termination to take effect at the end of the then-current Term.

Merger: If the Provider merges into another entity under English law where the Provider is not the surviving entity, the surviving entity shall provide written notice to the Client within thirty (30) days after the effective date of such merger.

SCHEDULE 1 (HOSTED SERVICES PARTICULARS)

Description of Hosted Services

3D Liveness

“Facia 3D Liveness service functions based on utilizing in-house state-of-the-art AI models for verifying a person’s liveness from their face image/video. Facia liveness detection service aims to provide a high level of accuracy. The liveness detection real-time journey is designed to enhance security measures by conducting various checks, including Print Attack, Replay Attack, 3D Mask Attack, Camera Manipulation, and Thermal Imaging Attack.

Face Match (1:1)

Face Match (1:1) feature enables businesses to cross-validate a single image with another image/video in real-time. AI models are capable of accurately detecting the similarity between two

provided face

images to identify potential fraud. This functionality can be applied for access control, authentication, or any situation necessitating a robust level of identity confirmation.

Face Enrol

With Face Enrol service, customers have the option to securely enrol face images into Facia's database.

The process includes storing images for potential identification purposes. This step is viewed as

essential in establishing a strong and dependable authentication system.

Face Search (1: N)

The Face Search (1: N) feature is designed to enhance identification capabilities by allowing the

system to search through a database for a potential match when presented with a facial image. This

feature can be useful in scenarios where identification from a pool of individuals is needed, such as in

public security, event management, or customer verification. The system will compare the provided face

image with all existing entries and may return a match if one is found.

Age Estimation

Age Estimation service leveraging advanced facial analysis algorithms offers a method to provide an

approximate estimation of an individual's age based on facial features, offering valuable insights.

Account deduplication

Facia offers the option to address data integrity challenges with its account deduplication service.

Through the use of facial recognition technology, the system is designed to identify and resolve

duplicate entries within accounts or databases. This service aims to assist clients in managing certain

risks in line with their business requirements and to limit access for users attempting multiple

verifications.

Client Infrastructure

The Client may, at their discretion, consider incorporating the Hosted Services into their respective

web platforms or mobile application interfaces

Financial Obligations

Notwithstanding any other provision contained herein, the Agreement shall become operational upon the

Client's payment of the setup fee and/or any ancillary Financial Obligations as set out in a valid Sales

Order, without implying any warranty or guarantee.

Authorized Representatives

The Client must ensure that any instructions related to the matters outlined in the Agreement are communicated solely by a designated Client Representative to a designated Provider Representative. The Provider is entitled:

to regard such instruction as being duly sanctioned by the Client; and
to refuse compliance with any divergent instructions pertaining to the same topic.

Notices

For the transmission of any contractual communications, the Client is required to communicate with the Provider via email at: legal@facia.ai

SCHEDULE 2 (AVAILABILITY SLA)

Scope

Schedule 2 outlines the Provider's responsibilities regarding the availability of the Hosted

Services in a contemporary manner.

Schedule 2 – Uptime Definition

Within the scope of this Schedule 2, the term "uptime" is defined as the measurable percentage

within a specified period where the Hosted Services are operational at the point where the public

internet connects with the Provider's network infrastructure.

Service Availability

Subject to Clause 4, 5 & 6:

The Provider is obligated to make all reasonable efforts to ensure that the Hosted Services

maintain an uptime of at least 99% for each calendar month.

The Provider is responsible for evaluating and measuring uptime, using any reasonable and fair method for such evaluation..

Upon the Client's written request, the Provider shall provide the Client with a report outlining

the uptime metrics for each month. This report must be delivered within ten (10) business days upon

receipt of the request from the Client.

Exemptions

Any service interruption or downtime, whether directly or indirectly caused by any of the listed

situations below, shall be excluded from the calculations determining the Provider's compliance with

the uptime commitment outlined in Paragraph 2.1:

a Force Majeure Event;

any disruption or failure in the Provider's hosting infrastructure operations;

any failure or disruption of the Client's digital devices or network systems;

any breaches by the Client of the provisions of the Agreement; or

periodic maintenance carried out in accordance with the Agreement.

SCHEDULE 3 (MAINTENANCE SLA)

Scope

This Schedule 3 sets out the service standards applicable to the Maintenance Services.

Scheduled Maintenance

Where commercially reasonable, the Provider will provide the Client with at least ten (10) Business

Days' advance written notice of any upcoming Maintenance Services that could impact the availability

or significantly and negatively impact the Hosted Services. This notice does not affect any other

notification requirements outlined in this Schedule 3..

The Provider will endeavor to perform all specified Maintenance Services outside of regular business hours, to the extent possible..

Updates

The Provider will provide the Client with a formal written notice regarding the implementation of any security Update on the Platform and must give a minimum of ten (10) Business Days' advance

written notice for the implementation of any non-security Update on the Platform..

The Provider's responsibilities regarding the implementation of Updates on the Platform are as follows:

Security updates from third-party sources will be promptly implemented on the Platform upon their release by the relevant third party. However, the Provider will use careful judgment in deciding not to apply certain third-party security updates..

The Provider will promptly integrate indigenous security updates into the Platform upon identifying a security vulnerability and successfully validating the relevant update..

Diverse Updates will to the extent feasible be seamlessly incorporated into the Platform in accordance with any timetable communicated by the Provider to the Client or mutually agreed upon by the parties on a regular basis.

Upgradation

At a minimum, during the Term, the Provider reserves the right to introduce Upgrades once in each calendar year.

To the extent commercially reasonable to do so, Provider will provide the Client with at least ten (10) Business Days' written notice before implementing an Upgrade on the Platform..

Each Upgrade to the extent commercially reasonable will be seamlessly incorporated into the Platform within a timeframe specified by the Provider to the Client or mutually

agreed upon in writing.

SCHEDULE 4 (SUPPORT SLA)

Scope

This Schedule sets out the service standards for the provision of Support Services.

Help Desk Provisions

The Provider agrees to provide the Client with a help desk in accordance with the terms set forth in this Schedule 4.

The Client may only use the help desk for seeking assistance and accessing the Support Services.

The Client is not allowed to use the help desk for any other purposes..

The Provider will use reasonable endeavors to ensure that the help desk is accessible through

email, the Provider's online chat platform, and, if these methods are unavailable, via phone or

Skype..

The Provider will use reasonable endeavors to ensure that the help desk is operational and

adequately staffed during business hours. Additionally, the Provider is required to provide a

telephone contact for the Client to address urgent matters outside of regular business hours..

The Client agrees to ensure that all requests for Support Services are directed solely through the

help desk..

Response and Remediation Protocols

Issues brought forth via the Support Services shall be classified (as determined by the Provider in

its discretion acting reasonably) as:

Urgent: The Hosted Services cease to function, or a core feature of the Hosted Services becomes

inaccessible;

Normal: A core feature of the Hosted Services encounters interference, which does not escalate to a critical issue; or an additional feature of the Hosted Services experiences significant disruption

The Provider agrees to use reasonable endeavors to ensure that its response to a request for Support Services includes the following information (if relevant to the request): confirmation of receipt of the request, an initial assessment of any reported issues, and a proposed timeline for addressing the request.

Support Levels

Support Type	Response Time, within within Business Days		Resolution Time, within Business Days
Basic	Normal:	3	5
	Urgent:	1	
Priority	Normal:	2	1
	Urgent:	1	

Stipulation for the Tendering of Support Assistance

The Support Services will be provided remotely, unless the parties mutually agree otherwise in writing..

Support Services Limitations

Notwithstanding the specific Support Category chosen by the Client, if the total hours worked by the Provider’s personnel in providing Support Services in any calendar month exceed twenty (20) hours,;

The Provider's obligation to provide Support Services to the Client for the rest of the current calendar month shall cease.;
the Provider may, in its sole discretion, agree to provide Support Services to the Client for the remaining part of the same calendar month, possibly subject to additional Charges. The Provider is not obligated to provide Support Services for any resulting discrepancies from:
the Client's unauthorized use of the Hosted Services; or
any changes to the Hosted Services made without the Provider's prior approval.

SCHEDULE 5 (DATA PROCESSING INFORMATION)

Categories of Data Subject

Client's Face data

Purposes of Processing

All Personal Data will be processed in accordance with our Privacy Policy, which can be accessed [here](#). The processing of Personal Data includes but is not limited to ensuring liveness, facial authentication, face matching, face search, and age estimation.

Security Measures for Personal Data

All pertinent data is conveyed utilizing Secure Sockets Layer (SSL) and is conserved within secure data repositories compliant with SSAE standards and accredited by ISO. All personal data is safeguarded with utmost precision utilizing either AES 256-bit encryption or SHA-256 cryptographic hash algorithm to

ensure paramount protection; moreover, TLS encryption is employed for the encryption of data during its transit phase.

Audit and Compliance

The Provider may, upon reasonable notice, audit the Client's use of the Hosted Services to verify compliance with this Agreement.