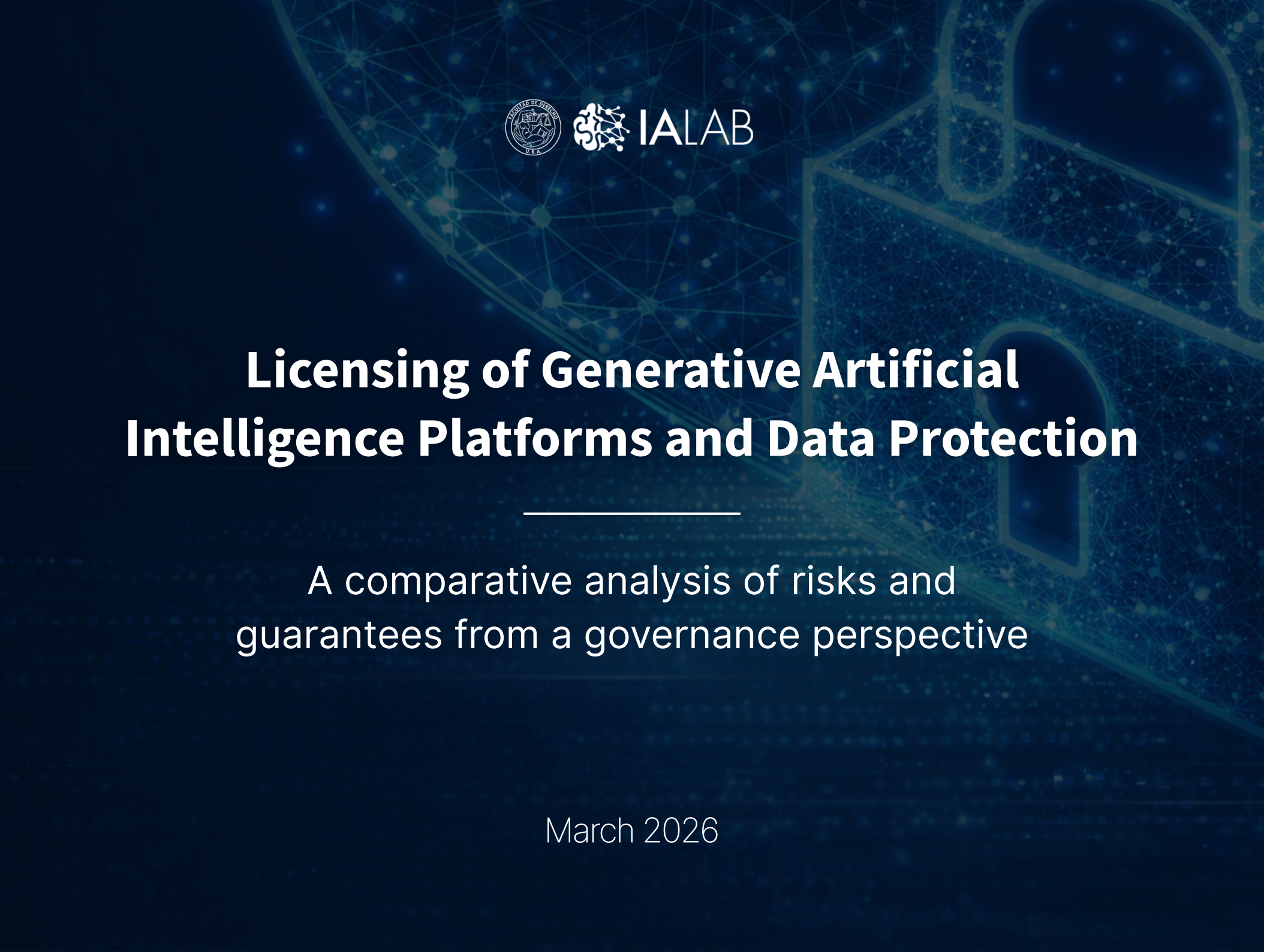

Licensing of Generative Artificial Intelligence Platforms and Data Protection

A comparative analysis of risks and guarantees from a governance perspective

March 2026

Grok

Plataform	Grok for individuals	Grok for commercial users	Grok API
Type of user	Consumer	Business	
Terms and Conditions (link)	https://x.ai/legal/terms-of-service	https://x.ai/legal/terms-of-service-enterprise	
	https://x.ai/legal/faq	https://x.ai/legal/enterprise/faq	
Privacy Policy (link and scope)	https://x.ai/legal/privacy-policy	https://x.ai/legal/data-processing-addendum	
	Our Privacy Policy describes how we collect, use, and disclose your personal information when you use our websites and applications (the Grok mobile app (iOS or Android) or the Grok.com website). This Privacy Policy does not apply to data we process on behalf of customers of our commercial offerings, such as the xAI API	The Data Processing Addendum, including its Appendices (the "DPA"), is incorporated into and forms part of the Enterprise Terms of Service ("Agreement") between the Customer (also known as "you") and xAI.	
Data Processing Agreement (DPA)	N/A	Yes. It provides that any person authorized to process Customer Data is subject to a duty of confidentiality. It does not disclose Customer Data to public bodies without legal order. The company has an obligation to notify incidents within 48 hours. It provides reasonable cooperation and assistance necessary to fulfill the customer's obligation to conduct impact assessments.	
Company warnings	We ask that you NOT include personal information in your prompts and inputs to our Service; however, we cannot control what you provide to us	The Customer agrees not to send, and will prohibit End Users from sending to the Services: (a) large volumes or routine personal data or information; (b) any information that includes or constitutes sensitive personal data under applicable privacy laws or other regulations; (c) "protected health information" as defined in the HIPAA Privacy Rule (45 CFR Section 160.103); or (d) financial data, such as data subject to the Payment Card Industry Data Security Standard (PCI DSS) requirements. If the Customer wishes to process such data, they must contact xAI and agree to the Enterprise Customer Agreement	
Data collection	Yes		

Plataform	Grok for individuals	Grok for commercial users	Grok API
Types of data collected	It collects different types of data. Account data: If you create an account, we will collect your name, contact information, account credentials, and date of birth. Payment data: when payment is required to access the Service. Communication data: If you communicate to request something in particular. User Content: when providing personal information in prompts and other content you enter, such as files, images, audio, voice, video, and other materials ("Input"). The Service's outputs ("Outputs"), including the responses that Grok generates, are based on your Input (collectively, "User Content"). If you include personal information in the Inputs you provide to the Service, this information may be reproduced in the Outputs.		
What information NOT to enter (as requested by the company)	They request that you do not provide sensitive personal information (e.g., information related to racial or ethnic origin, political opinions, religion or other beliefs, health, biometric scans, criminal history, or union affiliation).	It requests that you do not share medical information without having first signed a business associate agreement.	It does not comply with HIPAA (Health Insurance Portability and Accountability Act)
What does it consider personal information?	Personal data: any information defined as "personal information" under the CCPA, "personal data" under the GDPR, or other similar terms under applicable Data Protection Laws		
Data processing	To maintain and provide the Service. Product improvement and business purposes, through data analysis, market research, product and feature development, usage trends. Compliance and security. Use of automated systems to analyze usage and Content for security and compliance. Review by authorized personnel to improve the model, investigate incidents, prevent misuse, and fulfill legal obligations automatizados para analizar uso y Contenido para seguridad y cumplimiento. Revisión por personal autorizado para mejorar modelo, investigar incidentes, prevenir mal uso y cumplir obligaciones legales	Process Personal Data solely in accordance with your documented lawful processing instructions.	
Use of data for model training	Yes	It does not use enterprise customer content to improve its models.	
Training opt-out options	Upon logging in, you can choose whether your Content is used to train models and improve services. If you use the Service without an account, you give permission (where allowed) to use data for training. When temporary chat is used, data is not used for training.	Yes	
Does it share data?	The collected data may be shared with contracted service providers; in connection with business transfers, for legal purposes (to comply with laws or respond to legal requests and legal processes); and with its related companies.	It is ensured that any person authorized to process Personal Data is subject to a duty of confidentiality. Government requests: We will not disclose Personal Data to any law enforcement agency or governmental authority (collectively, the "Governmental Authority") unless you direct us to or when necessary to comply with applicable law or a valid and binding order from a Governmental Authority, such as a subpoena or court order. If we are legally compelled to respond to a request from a Governmental Authority, we will review the legality of the request and determine whether it can be challenged. In any case, we will only disclose the minimum information necessary to comply with the request.	

Plataform	Grok for individuals	Grok for commercial users	Grok API
Sale of information for commercial purposes	They do not sell or use your personal information for marketing purposes: They do not sell or share personal information for targeted advertising or cross-contextual purposes.		
International data transfer	Data may be processed in the US	xAI may transfer and process Personal Data outside of Europe, as necessary for the provision of the Service, including the United States and other countries where xAI and its Sub-processors conduct data processing operations.alizan operaciones de procesamiento de datos.	
Data retention	Temporary and deleted chat content is stored for up to 30 days before deletion. Information is retained when there is a legitimate and ongoing business need that requires them to do so (for litigation, security, among other reasons).	Upon termination of the Agreement, we will delete any Personal Data in our possession, in accordance with the Agreement, unless we are required to retain copies under applicable law. In that case, we will isolate and protect such Personal Data from any further processing, except to the extent required by applicable law.	They are stored on their servers for 30 days in case they need to be audited to detect possible abuse or misuse. This data is automatically deleted after 30 days.
Security measures	Yes. They implement commercially reasonable technical, administrative, and organizational measures designed to protect personal information against loss, misuse, and unauthorized access, disclosure, alteration, or destruction.	Various technical and organizational measures are adopted to ensure an adequate level of security, taking into account the nature, scope, context, and purpose of the processing, and form an integral part of the Agreement. They are described in the DPA.	All API requests and responses are encrypted in transit and at rest using AES256.
Advertisements	No		
Legal protection for users	Si. Vía contacto en https://xai-privacy.relyance.ai/	Yes. Direct contact lines for commercial customers: security@x.ai o support@x.ai.	

OpenAI

Platform	ChatGPT Free	ChatGPT Go	ChatGPT Plus	ChatGPT Pro	ChatGPT Business	ChatGPT Enterprise	OpenAI API
Type of user	Consumer				Enterprise		
Terms and Conditions (link)	https://openai.com/es-ES/policies/terms-of-use/				https://openai.com/policies/business-terms/		
	https://openai.com/es-ES/consumer-privacy/				https://openai.com/policies/service-terms/		
Privacy Policy (link and scope)	https://openai.com/es-ES/policies/row-privacy-policy/				https://openai.com/enterprise-privacy/		
					https://openai.com/policies/data-processing-addendum/		
	This Privacy Policy does not apply to content we process on behalf of customers of our Business offerings, such as our API. Our use of that data is governed by agreements with our customers covering access to and use of those offerings.				The use of that data from customers of our Business offerings, such as our API, is governed by agreements with our customers covering access to and use of those offerings. It offers ownership and control over your company's data.		
Data Processing Agreement (DPA)	N/A				Yes. We can add a data processing addendum (DPA) with customers for their use of ChatGPT Business, ChatGPT Enterprise, ChatGPT Edu, and the API to support their compliance with the GDPR and other privacy laws. We can also sign business associate agreements to support customers' compliance with the US Health Insurance Portability and Accountability Act (HIPAA). OpenAI and the Customer will comply with the DPA, which is incorporated by this reference into the Agreement.		
Company warnings	Not informed				The Customer agrees not to use the Services to create, receive, maintain, transmit, or otherwise process Protected Health Information, unless they have signed the Healthcare Addendum.		
Data collection	Yes						
Types of data collected	It collects different types of data. Account information: data related to the account (name, contact information, date of birth, account credentials, payment data, and transaction history). User content: We collect Personal data that you provide in the inputs to our Services ("Content"), which includes instructions and other content you upload, such as files, images, and audio, depending on the features you use.						
What information NOT to enter (as requested by the company)	They have restrictions on generated content, prohibiting use for illegal, harmful activities, or activities that infringe intellectual property rights.				Content restrictions apply, prohibiting illegal, harmful uses, or those that infringe intellectual property rights, with greater control depending on the plan.		

Platform	ChatGPT Free	ChatGPT Go	ChatGPT Plus	ChatGPT Pro	ChatGPT Business	ChatGPT Enterprise	OpenAI API
What does it consider personal information?	Personal information includes any data that can identify a person, such as names, addresses, phone numbers, emails, etc.						
Data processing	They may use personal data to: provide, analyze, and maintain Services; improve and develop Services and conduct research, (for example, to develop new product features); communicate with the user; prevent fraud, illegal activities, or misuse of their Services, and protect the security of systems and Services; comply with legal obligations and protect the rights, privacy, security, or property of users, OpenAI, or third parties.				OpenAI will only process Customer Data for the provision of Services to the Customer in accordance with the Agreement and the DPA. OpenAI will only use Customer Content as necessary to provide you with the Services, comply with applicable law, enforce OpenAI's Policies, and prevent abuse. OpenAI will not use Customer Content to develop or improve the Services, unless the Customer explicitly agrees to it. We may process any business data submitted to OpenAI services through automated content classifiers and security tools, for example, to better understand how our services are used. The classifications created are metadata about the business data, but do not contain any of this data itself. Business data is only subject to human review: for ChatGPT Edu and Enterprise, authorized OpenAI employees will only access conversations to resolve incidents and retrieve end user conversations with your explicit permission or when required by applicable law; in ChatGPT Business, our access to conversations stored in our systems is limited to the following persons: (1) authorized employees who require access for technical support purposes, investigation of potential platform abuse, and legal compliance, and (2) specialized external contractors who are subject to confidentiality and security obligations, solely for abuse and misuse evaluation purposes. OpenAI commits not to "sell" (as defined by US Privacy Laws) or "share" (as defined by the CCPA) Personal Data.		
Use of data for model training	They may use the content you provide to improve Services, for example, to train the models that power ChatGPT, unless users opt out of this option in settings or use temporary chat.				They are trained using machine learning techniques on large volumes of textual data.		
Training opt-out options	Yes				OpenAI does not use customer data to train its models. Your input and output data are your property (when permitted by law). You control how long data is retained (ChatGPT Enterprise). You control which internal sources are connected (ChatGPT Business and Enterprise).		

Platform	ChatGPT Free	ChatGPT Go	ChatGPT Plus	ChatGPT Pro	ChatGPT Business	ChatGPT Enterprise	OpenAI API
Does it share data?	They may disclose your Personal data in the following circumstances. Vendors and service providers to help us meet our business needs and develop certain services and features (including hosting service providers, as well as customer service providers, cloud service providers, content delivery providers, security support and monitoring providers, email communication software providers, web analytics providers, payment and transaction processing providers, and other IT service providers). Business transfers, in the event that they are subject to a strategic transaction, reorganization, bankruptcy proceeding, payment suspension, or transfer of services to another provider, Personal data may be disclosed in the due diligence process to counterparties and third parties collaborating in the Transaction and transferred to a successor or affiliated entity as part of such Transaction, along with other assets. Government authorities or other third parties, they may share your Personal data, including information about your interaction with our Services, with government authorities, industry companies, or third parties in accordance with applicable regulations: i) if required by applicable law or if we believe in good faith that such action is necessary to comply with a legal obligation; ii) to protect and defend our rights or property; iii) if we determine, at our sole discretion, that there has been a breach of our terms, policies, or the law; iv) to detect or prevent fraudulent or illegal activities; v) to ensure the safety and integrity of our products, employees, users, or the public; or vi) to protect ourselves against any legal liability. Affiliated entities, they may disclose Personal data to affiliated entities.				No		
Sale of information for commercial purposes	It is not clarified.						
International data transfer	OpenAI does not publicly specify the exact locations of the servers used to process data in ChatGPT Free, ChatGPT Plus, and ChatGPT Pro. However, it is known that the company operates primarily in the United States.			OpenAI processes data on global servers, including the United States and Europe, through platforms such as Microsoft Azure.			
Data retention	No fixed public period is specified, but it states "...how long we retain Personal data depends on the type of data, how we use it..." and, in certain cases, on user settings. That is, it depends on various generically stated factors. Temporary chat data is deleted after 30 days.				Each of the end users controls whether their conversations are retained. Any deleted or unsaved conversation is removed from our systems within 30 days, unless we are legally required to retain it		OpenAI may securely retain API input and output data for up to 30 days to provide its services and identify abuse. After 30 days, API input and output data are deleted from our systems unless we are legally required to retain them. You can also request data non-retention for eligible endpoints if you have a valid use case.

Característica/Plataforma	ChatGPT Free	ChatGPT Go	ChatGPT Plus	ChatGPT Pro	ChatGPT Business	ChatGPT Enterprise	OpenAI API
Security measures	We implement commercially reasonable technical, administrative, and organizational measures to protect Personal data against any loss, misuse, and unauthorized access, disclosure, alteration, or destruction.				OpenAI encrypts all data at rest (AES-256) and in transit between our clients and us, and between our providers and us (TLS 1.2+) and uses strict access controls to limit who can access the data. Our security team has a shift rotation to provide 24/7/365 coverage and their assistance is requested in the event of a potential security incident. The API platform has been audited and has SOC 2 Type 2 compliance certification. ChatGPT Business has successfully passed the SOC 2 Type 2 audit.		
Advertisements	Yes. In the US for now. We do not share your ChatGPT conversations with advertisers or sell them your data. Advertisers do not have access to your chats, chat history, memories, or personal data. They only receive aggregated and non-identifiable information about the performance of their ads, such as total views or clicks. Ads will be personalized based on your chats and the context that ChatGPT uses to respond to you. If memory is enabled, ChatGPT may save and use memories, as well as consult recent chats, when selecting an ad. ChatGPT Free		No				
Legal protection for users	Yes. You can exercise your rights through your OpenAI account. If you cannot exercise your rights through your account, submit a request through privacy.openai.com (opens in a new window) or to dsar@openai.com. You can contact our data protection officer at privacy@openai.com. If you notice that ChatGPT results contain inaccurate information about you and want to request a correction or deletion of the information, you can submit these requests through privacy.openai.com or to dsar@openai.com. Also through: https://privacy.openai.com/policies/en/				Notifications to OpenAI must be sent to OpenAI Legal at the address contract-notices@openai.com, with a copy to: (a) if it concerns OpenAI, LLC, 1455 3rd Street, San Francisco, California 94158; or (b) if it concerns OpenAI Ireland Ltd, 1st Floor, The Liffey Trust Centre, 117-126 Sheriff Street Upper, Dublin 1, D01 YC43, Ireland.		

IALAB

Google

Plataform	GeminiApp	Gemini API in Google Studio (free service)	Gemini API in Google Studio (paid service)
Type of user	Consumer	Enterprise	
Terms and Conditions (link)	https://policies.google.com/?hl=en	https://developers.google.com/terms	
		https://ai.google.dev/gemini-api/terms?hl=es-419	
Privacy Policy (link and scope)	https://x.ai/legal/privacy-policy	https://x.ai/legal/data-processing-addendum	https://business.safety.google/processorterms/
	This notice supplements Google's Privacy Policy and explains how Google processes your data when you interact with Gemini.	https://business.safety.google/processorterms/?hl=es-419	
		All Services offered at no cost, such as direct interactions with Google AI Studio or the unpaid tier of the Gemini API, are Unpaid Services (the "Unpaid Services").	When a Service is offered for a fee, it is considered a Paid Service (the "Paid Services"). When you activate a Cloud Billing account, all use of the Gemini API and Google AI Studio is considered a "Paid Service" with respect to how Google Uses your Data, even when you use Services offered at no cost, such as Google AI Studio and the free tier of the Gemini API.
Data Processing Agreement (DPA)	Google restricts access to personal information to Google employees, contractors, and agents who need it to process it. Anyone with this access is subject to strict contractual confidentiality obligations and could be sanctioned or dismissed if they do not comply with these obligations.	Yes, there is an agreement to process user data in the Google API for developers in the form of the Google Controller-Controller Data Protection Terms, but this is not a typical data processing agreement (DPA) where Google acts as a processor. Instead, it is an agreement between independent controllers that regulates how Google and the developer handle personal data, each with their own responsibilities and purposes, subject to applicable data protection laws.	There is a formal agreement between Google (as data processor) and the customer (as data controller) to define: Google's obligations when processing "Personal Data" on behalf of the customer. The customer's rights over their data. Security measures, subprocessing, and compliance with regulations such as the GDPR.

Plataform	GeminiApp	Gemini API in Google Studio (free service)	Gemini API in Google Studio (paid service)
Company warnings	Do not enter confidential information that you do not want a reviewer to see or that Google uses to improve its services, including machine learning technologies.	You may not use the Services in clinical practice, to provide medical advice, or in any other way that must be supervised, authorized, or approved by a medical device regulatory body. Do not submit personal, sensitive, or confidential information to Unpaid Services. See also prohibitions at: https://policies.google.com/terms/generative-ai/use-policy?hl=es-419 (prohibited use policy)	
Data collection	Yes	Yes	
Types of data collected	Google collects personal information, such as name and password. It may also add phone number or email. It also collects What you tell Gemini Apps (such as the instructions you send or say). What you share with Gemini Apps (such as files, videos, screens you ask about, photos, and content from pages you share from your browser). Transcripts and recordings of your interactions with Gemini Live (including audio, videos, and screens you share with Live). Your feedback. Names and personalized instructions for your Gems. Instructions for Gemini (or "Saved Information" in some languages). The content generated by Gemini Apps (such as text, code, audio, images, videos, public links, quotes, chat summaries, and personalized statistics). Information from your apps, browsers, and devices. Information from your connected apps and other Google services you use with Gemini Apps (such as your Search or YouTube history, or the context and URL of pages you share from Chrome).	They include messages, files, data specific to Google users (with consent), data submitted by the developer, and technical usage data.	
What information NOT to enter (as requested by the company)	They have restrictions on generated content, prohibiting use for illegal, harmful activities, or activities that infringe intellectual property rights.	Data for which the user has not given explicit consent. Data not requested by the developer through the API. Data processed locally without transmission to Google. Data not necessary for the intended functionality of the application. Data restricted by additional applicable laws or policies.	
What does it consider personal information?	Personal information refers to any data that can identify you, either directly or indirectly.	Information linked to a Google user that requires consent for access (such as messages, files, or data specific to their account). Sensitive data that must be protected against unauthorized use or access (such as identifiers or personal content). Any data that falls under the definitions of applicable privacy laws, including direct or indirect identifiers and user-generated content.	

Plataform	GeminiApp	Gemini API in Google Studio (free service)	Gemini API in Google Studio (paid service)
Data processing	Google uses this data, as described in our Privacy Policy, to: provide our services; maintain and improve our services; develop new services; personalize our services (more information); adapt our services; communicate with you; measure performance; protect Google, our users, and the public. These uses extend to generative AI models and other machine learning technologies that power our services. Our human reviewers (including trained reviewers from our service providers) analyze some of the data we collect for these purposes.	When you use Unpaid Services, including, for example, Google AI Studio and the unpaid tier of the Gemini API, Google uses the content you submit to the Services and the generated responses to provide, improve, and develop its products and services, as well as its machine learning technologies, including Google enterprise products, features, and services.	When you use Paid Services, including, for example, the paid tier of the Gemini API, Google does not use your prompts (which include system instructions, cached content, and files such as images, videos, or documents associated) or responses to improve our products, and will process your prompts and responses in accordance with the Data Processing Addendum for Products in which Google is a Data Processor. For Paid Services, Google stores prompts and responses for a limited period, solely for the purpose of detecting violations of the Prohibited Use Policy and any necessary legal or regulatory disclosure. This data may be stored transiently or cached in any country where Google or its agents have facilities.
Use of data for model training	Yes, it uses the data provided by the user to train and improve the model.	To improve quality and our products, human reviewers may read, label, and process both the inputs you make to the APIs and the outputs derived from them. Google takes measures to protect your privacy as part of this process. This includes unlinking the data from your Google Account, API key, and Cloud project before reviewers see or label it. Do not submit personal, sensitive, or confidential information to Unpaid Services.	When you use Paid Services, including, for example, the paid tier of the Gemini API, Google does not use your prompts (which include system instructions, cached content, and files such as images, videos, or documents associated) or responses to improve our products.
Training opt-out options	The user can choose to mark their inputs or outputs as not usable for training.	N/A	
Does it share data?	Google does not share personal information with companies, organizations, or individuals except in the following cases: With consent: If the user gives explicit permission to share the data. With partners or data processors: Google works with affiliates and third parties (such as service providers) that process data on its behalf, but these are subject to agreements that protect the information. For legal reasons: If required by law, a court order, or to protect the rights, property, or safety of Google, its users, or others. Within Google: Data may be shared between Google services and entities to operate and improve products.	Yes, it shares. In "data portability" it states that "While you use or store user data obtained through the APIs, you agree to allow your users to export their equivalent data to other services or applications of their choice in a manner practically as fast and easy as exporting them from Google's products and services, subject to applicable law, and you agree not to share such data with third parties who do not comply with this obligation." It also establishes that if the developer wishes to access Google user data, they must specify what data they request, who requests it, and why they request it.	
Sale of information for commercial purposes	Your Gemini Apps conversations are not being used to show you ads. If this changes, we will clearly inform you.	They are not used	

Plataform	GeminiApp	Gemini API in Google Studio (free service)	Gemini API in Google Studio (paid service)
International data transfer	Global location: Google processes data on servers located around the world, which means that information (such as the "Input" and "Output" from the Gemini API) "may be processed on servers located outside the country where the user lives." This includes the United States and other countries where Google or its affiliates and partners have facilities.		
Data retention	You can change the auto-delete setting parameter in Activity in Gemini Apps. The default period is 18 months, but you can change it to 3 months, 36 months, or an indefinite period. You can also manually delete your Gemini Apps chats at any time. Chats reviewed by human reviewers (and related data, such as your language, device type, location information, or feedback) are not deleted when you delete your activity, but are retained for up to three years. We retain some data until you delete your Google Account, such as information about how frequently you use Gemini Apps. We retain some data for longer when necessary for legitimate legal or business reasons (for example, to prevent abuse or fraud, ensure security, or maintain accounting records).	Google's API states that "Google will store prompts, context information you provide, and outputs for thirty (30) days to create Grounded Outputs and Search Suggestions, and the stored information may be used to debug and test the systems that support Grounding with Google Search."	
Security measures	Google uses encryption to keep data private while in transit. Google offers a variety of security features, such as Safe Browsing, Security Checkup, and Two-Step Verification, to protect the account. Google reviews its information collection, storage, and processing practices, including physical security measures, to prevent unauthorized access to its systems. Google restricts access to personal information to Google employees, contractors, and agents who need it to process it. Anyone with this access is subject to strict contractual confidentiality obligations and could be sanctioned or dismissed if they do not comply with these obligations.	Google will implement and maintain technical and organizational measures to protect Partner Personal Data against destruction, loss, alteration, unauthorized disclosure or access, whether accidental or unlawful.	
Advertisements	No		
Legal protection for users	Redirects to the Privacy Help Center https://support.google.com/policies/answer/9581826?p=privpol_privts&hl=en&visit_id=638794910213455178-1640318101&rd=1	Redirects to the Privacy Help Center https://support.google.com/policies/answer/9581826?p=privpol_privts&hl=en&visit_id=638794910213455178-1640318101&rd=1 Contact with Google. The Partner may contact Google to exercise their rights under this Data Processing Addendum at legal-notices@google.com or through other means that Google may provide.	

Claude

Plataform	Individual Claude (Claude Free, Pro, Max)	Claude for Work	Claude API
Type of user	Consumer	Enterprise	Enterprise
Terms and Conditions (link)	https://www.anthropic.com/legal/consumer-terms	https://support.anthropic.com/es/collections/9387370-claude-para-el-trabajo-plan-de-equipo-y-empresa	https://docs.anthropic.com/en/docs/resources/api-features
Privacy Policy (link and scope)	https://www.anthropic.com/legal/privacy	https://www.anthropic.com/legal/privacy https://docs.anthropic.com/en/docs/resources/api-features https://docs.anthropic.com/en/docs/resources/api-features	
	This Privacy Policy explains how we collect, use, disclose, and process your personal data when you use our website and other places where Anthropic acts as a data controller; for example, when you interact with Claude.ai or other products as a consumer for personal use ("Services") or when Anthropic operates and provides our business customers and their end users with access to our business products, such as the Claude Team plan ("Business Services"). The Data Processing Addendum (DPA) is incorporated into and forms part of Anthropic's Commercial Terms of Service or other agreement between the Customer and Anthropic that references this DPA and governs the Customer's use of the Services (the "Agreement"), and applies to Anthropic's processing of Customer Data (defined below).		
Data Processing Agreement (DPA)	It does no mention	Yes, there is an explicit agreement on data processing which is the "Data Processing Addendum" (DPA). This document applies to Anthropic's commercial services (such as Claude for enterprises) and is designed to comply with data protection regulations such as the GDPR. Anthropic's Data Processing Addendum (DPA) with Standard Contractual Clauses (SCCs) is automatically incorporated into our Commercial Terms of Service. By accepting Anthropic's Commercial Terms of Service, you also accept our DPA.	
Company warnings	It does no mention		
Data collection	Yes		

Plataform	Individual Claude (Claude Free, Pro, Max)	Claude for Work	Claude API
Types of data collected	Identity and contact data: identifiers, such as your name, email address, and phone number, when you create an Anthropic account or to receive information about our Services. We may also collect or generate indirect identifiers (e.g., "USER12345"). Payment information: We will collect your payment information if you choose to purchase access to Anthropic's products and services. Inputs and Outputs: You may interact with our Services in various formats, including but not limited to chat, programming, and agency sessions ("Prompts" or "Inputs"), which generate responses and actions ("Outputs") based on your Inputs. This includes third-party applications that you choose to integrate with our Services. If you include personal data or reference external content in your Inputs, we will collect such information and it may be reproduced in your Outputs. Feedback on your use of our Services: We appreciate your feedback, including ideas and suggestions for improvement, or rating an Output in response to an Input ("Feedback"). If you rate an Output in response to an Input (for example, using the thumbs up or thumbs down icon), we will store the entire related conversation as part of your Feedback. You can learn more about how we use Feedback here. Communication information: if you communicate with us, including through our chatbot on our Help site, we collect your name, contact information, and the content of any message you send.	Personal data provided directly: Identity and contact data Payment information Inputs and Outputs Feedback on your use of the Services Communication information Personal data that Claude receives automatically: Device and connection information Usage information Logging and troubleshooting information Cookies and similar technologies	
What information NOT to enter (as requested by the company)	It does no mention		
What does it consider personal information?	The Privacy Policy (Section 1: "Information we collect") implicitly defines "personal information" as any data that can identify an individual. Although there is no explicit definition with that exact term, the examples provided include: Name and email address (provided when creating an account or communicating with Anthropic). IP address (automatically collected as part of device information). Usage data that may be linked to an individual (such as specific interactions with the services, if associated with an account). Content of communications with Anthropic (for example, support emails or messages).	According to Anthropic's "Privacy Policy," personal information (or "personal data") is defined as any data that can identify an individual, either directly or indirectly.	

Plataform	Individual Claude (Claude Free, Pro, Max)	Claude for Work	Claude API
Data processing	To provide, maintain, and facilitate any product and service offered to you with respect to your Anthropic account, which are governed by our Terms of Service; to provide, maintain, and facilitate optional services and features that enhance platform functionality and user experience; to communicate with you, including to send you information about our Services and events; to create and manage your Anthropic account; to facilitate payments for products and services provided by Anthropic; to prevent and investigate fraud, abuse, and violations of our Usage Policy, illegal or criminal activities, unauthorized access or use of personal data or Anthropic systems and networks, to protect our rights and the rights of others, and to comply with legal, governmental, and institutional policy obligations; to investigate and resolve disputes; to investigate and resolve security issues; to debug and identify and repair errors affecting existing functionality; to improve the Services and conduct research, including training our models; and to enforce our Terms of Service and similar terms and agreements, including our Usage Policy.	Anthropic will only process Customer Personal Data to provide or maintain the Services, and in compliance with the Customer's documented instructions (including as set forth in the Agreement and this DPA). Anthropic will not "sell" or "share" Customer Personal Data, as defined by Applicable Data Protection Laws; retain, use, or disclose Customer Personal Data outside the direct business relationship and for any purpose other than the business purposes specified in Part B of Annex 1 or as permitted by Applicable Data Protection Laws; and except as otherwise permitted by Applicable Data Protection Laws, may not combine Customer Personal Data with personal data that Anthropic receives from or on behalf of another person or persons, or that it collects from its own interaction with the data subject.	
Use of data for model training	Yes	Anthropic does not share its users' data with third parties for commercial purposes nor uses it to train its AI models, unless explicitly stated otherwise in a specific agreement.	
Training opt-out options	User-provided data is used to train the models unless you opt out in your account settings. Even if you opt out, we will use your Inputs and Outputs to improve the models when: (1) your conversations are flagged for safety review in order to improve our ability to detect harmful content, enforce our policies, or drive AI safety research, or (2) you have explicitly informed us about the materials (for example, through our feedback mechanisms).	N/A	

Plataform	Individual Claude (Claude Free, Pro, Max)	Claude for Work	Claude API
Does it share data?	Yes, Anthropic shares data with affiliates and corporate partners; service providers and business partners for various business purposes, such as website and data hosting, ensuring compliance with industry standards, research, auditing, data processing, and service provision. Anthropic may also disclose personal data in the following circumstances: as part of a major corporate event, if it participates in a merger, corporate transaction, bankruptcy, or other situation involving the transfer of business assets, Anthropic will disclose your personal data as part of these corporate transactions. In accordance with regulatory or legal requirements, security, third-party rights, and to enforce our rights or our terms. We may disclose personal data to government regulatory authorities as required by law, including for legal, tax, or accounting purposes, in response to their requests for such information, or to assist in investigations. We may also disclose personal data to third parties in connection with claims, disputes, or litigation, when permitted or required by law, or if we determine that its disclosure is necessary to protect your health and safety or that of any other person, to protect against fraud or credit risk, to enforce our legal rights or those of third parties, to enforce contractual commitments you have made, or as permitted or required by applicable law. With the person's consent. Anthropic will disclose personal data when a person gives us permission or instructs us to do so, including as part of our Services.	Anthropic does not share its users' data with third parties for commercial purposes nor uses it to train its AI models, unless explicitly stated otherwise in a specific agreement. In response to government requests for information, if data from an API or enterprise customer is requested, we will generally ask the requester to contact our customer in the first instance. As a rule, it does not disclose information about customers or end users of our services in response to government requests, except in accordance with a valid legal process (for example, a validly issued subpoena or court order).	
Sale of information for commercial purposes	It does no mention	It is expressly mentioned that not in the DPA	
International data transfer	By accessing our website or our Services, your personal data could be transferred to our servers in the US or other countries outside the European Economic Area (EEA) and the United Kingdom. This could consist of providing us with your personal data directly or a transfer that we or a third party make.	We may process customer data in selected countries in the US, Europe, Asia, and Australia, and store it in data centers located in the United States, unless otherwise agreed. Any changes to customer data processing locations will only be implemented after notifying them.	

Plataform	Individual Claude (Claude Free, Pro, Max)	Claude for Work	Claude API
Data retention	Anthropic conserva los datos personales de una persona durante el tiempo que sea razonablemente necesario para los fines y criterios establecidos en su Política de privacidad, detallados en su centro de privacidad. Cuando ya no se necesiten, tanto Anthropic como sus proveedores de servicios los destruirán, eliminarán, borrarán o anonimizarán conforme a las leyes aplicables. Si nos permite usar sus chats o sesiones de programación para mejorar Claude, podremos conservar sus datos de forma anónima durante un máximo de 5 años en nuestros procesos de entrenamiento de modelos.	Custom data retention controls allow organizations to manage how long Claude stores conversation and project data (minimum 30 days and does not apply to the API). For API users, we automatically delete inputs and outputs on our backend within 30 days of their receipt or generation, except for exceptions referenced in https://support.claude.com/es/articles/9796617-puedes-eliminar-los-datos-que-envie-a-traves-de-los-planes-team-y-enterprise. Anthropic retains personal data for as long as reasonably necessary (the default minimum is 30 days). Within thirty (30) days following the termination or expiration date of the Agreement, Anthropic will: if requested by the Customer within that period, return a copy of all Customer Data under its control or possession or provide self-service functionality that allows the Customer to do the same; and delete all copies of Customer Data (including Customer Personal Data) processed by Anthropic or any Subprocessor, with exceptions expressly referenced in the DPA. If you have provided us with feedback (for example, by submitting your comments through the "Like" or "Dislike" button or by submitting bug reports), we retain the data associated with such feedback for 5 years. Some enterprise API customers, subject to Anthropic's approval, may have agreements that allow them not to store their input or output data (zero retention), except when necessary to comply with the law or combat misuse.	
Security measures	Anthropic uses "reasonable technical and organizational measures" to protect collected information against unauthorized access, loss, or misuse. Specific measures (such as encryption or multi-factor authentication) are not detailed, but it is emphasized that security is a priority. The Commercial Terms (Section 7: "Security") also mention that Anthropic will implement "commercially reasonable measures" to protect customer data, and the Consumer Terms (Section 8: "Security") reiterate this commitment.	Anthropic uses industry-standard encryption methods for customer data protection, including a minimum of AES-256 for data at rest and TLS1.2+ for data in transit over public networks. It also maintains a robust set of internal security policies that are communicated and distributed to all staff (see DPA).	
Advertisements	No		
Legal protection for users	To exercise your rights, you or an authorized agent may submit a request by email to privacy@anthropic.com	privacy@anthropic.com	

IALAB

Mistral

Plataform	Mistral Le Chat o Le Plateforme	API and business clients
Type of user	Consumer	Enterprise
Terms and Conditions (link)	https://legal.mistral.ai/terms/privacy-policy?language=es-ES	https://legal.mistral.ai/terms/data-processing-addendum
Privacy Policy (link and scope)	It applies when you use our Mistral AI generative AI products, such as Le Chat or La Plateforme. This Privacy Policy does not apply if you use our Mistral AI Products to process personal data in the context of your business activities.	The Data Processing Addendum (the "Data Processing Addendum" or the "DPA") forms part of and supplements the Agreement entered into between Mistral AI and the Client as of the Effective Date..
Data Processing Agreement (DPA)	No	
Company warnings	You must not use Mistral AI Products to participate in, encourage, promote, offer, or solicit illegal activities, and any such use may be reported to law enforcement. Mistral AI has a zero-tolerance policy regarding child sexual abuse material. You must not use Mistral AI Products to generate intimate images of any person without the explicit consent of all persons involved. You must not use our Mistral AI Products to promote hatred, discrimination, or harassment, including the generation of any content that promotes, incites, glorifies, or celebrates hatred. Nor for fraud, misinformation, or professional advice.	
Data collection	Yes	
Types of data collected	Identifying data such as your first and last name. Account data, such as the means to recover your password and verify your account. Contact data, such as your email address. Contract data, such as the Mistral AI Product to which you subscribe. Payment and billing information. Input, any data you provide to generate an Output, such as prompts or fine-tuning data. Feedback, any information you provide when rating an Output, such as "like" or "dislike," and the associated Input and Output.	
What information NOT to enter (as requested by the company)	It does not mention	
What does it consider personal information?	Categories of personal data: Technical data: any record or technical data that your browser and device automatically send when you use Mistral AI Products, such as your IP address or the type of network protocol you use. Cookies listed in the privacy policy. Usage data, any data related to your use of Mistral AI Products. Output: any content generated by Mistral AI Products from your Input.	

Plataform	Mistral Le Chat o Le Plateforme	API and business clients
Data processing	To provide and maintain the Mistral AI Products that are supplied to you under the conditions set forth in our Terms of Service and any applicable Additional Terms. To improve your experience in Le Chat through the Memory feature, providing you with more relevant and personalized responses based on your previous interactions with Le Chat. To provide customer support, including debugging and correcting errors that you have reported. To improve Mistral AI Products or develop new products (but excluding model training), such as to conduct research or produce aggregated and anonymous statistics. To train our artificial intelligence models (large language models) to answer questions, generate text, translate, summarize and correct text, classify text, analyze sentiments, etc., according to context, Inputs (emails, letters, reports, computer code, etc.), and Output. To manage and enforce our Terms of Service and licenses, including moderation and abuse monitoring.	Process Personal Data solely in accordance with the Client's documented lawful instructions, including as set forth in this DPA or in the Agreement. Ensure that any person that Mistral AI authorizes to process personal data (including Mistral AI team members and subprocessors) is subject to a duty of confidentiality. Comply with all obligations applicable to it in its role as Processor under the Applicable Data Protection Law and provide the same level of privacy protection as required by the Applicable Data Protection Law.
Use of data for model training	Yes. It uses your Input and Output, subject to your opt-out. Please note that we do not use your Input and Output to train our artificial intelligence models when you use Le Chat Team, Le Chat Enterprise, or the paid version of our APIs.	We do not use your Input and Output to train our artificial intelligence models when you use Le Chat Team, Le Chat Enterprise, or the paid version of our APIs.
Training opt-out options	Yes. The user can opt out of their use.	
Does it share data?	Yes, it mentions that they may share your data with Financial institutions. Banks and other financial organizations. Regulatory authorities. Such as the French data protection authority (CNIL). Legal and professional services. When appropriate, we may share data with competent courts, mediators, accountants, auditors, lawyers, judicial agents, and debt collection agencies. Additionally, we may share all or part of your personal data with our service providers.	Mistral AI shall not: (i) Process Personal Data for a commercial purpose other than that necessary to provide Mistral AI Products to the Client; (ii) "sell" or "share" (each as defined by the CCPA) any Personal Data; (iii) Process Personal Data outside the direct business relationship between the Processor and the Client; or (iv) combine Personal Data with any other data or personal information it collects (directly or through a third party) except as expressly permitted by the Applicable Data Protection Law for Processors.
Sale of information for commercial purposes	It does not mention	No, it arises implicitly from the DPA.
International data transfer	We prioritize selecting providers within the European Union that strictly comply with the GDPR. However, in exceptional cases, we may opt for providers located outside the EU that meet our high standards of data security and personal data protection. We take the necessary measures to ensure that all contracts with service providers that process personal data outside the European Union include appropriate safeguards, in accordance with Article 46 of the GDPR.	

Plataform	Mistral Le Chat o Le Plateforme	API and business clients
Data retention	We store your personal data only for as long as necessary. Data we use to provide you with Le Chat: we retain your Input and Output until you delete your account or until you delete the Le Chat conversation.	Except in the case of specific APIs, we retain your Input and Output for the period necessary to generate the Output and then for thirty (30) consecutive days to monitor potential abuse (unless zero data retention is activated). If you use our Agents API, we retain your Input and Output until you cancel your account. If you use our Fine-Tuning API, we retain your fine-tuning data until you delete it from La Plateforme or until you cancel your account. Following the termination of the provision of Mistral AI Products, Mistral AI will delete or return to the Client all Personal Data Processed on their behalf, in accordance with its deletion policies and procedures. The Client acknowledges that Personal Data will cease to be accessible once thirty (30) days have elapsed since the termination of access and use of Mistral AI Products.
Security measures	See at: https://trust.mistral.ai/	
Advertisements	No	
Legal protection for users	https://mistral.ai/contact	You can contact us at any time through the chatbot available in our Help Center or by writing to support@mistral.ai


FACULTAD DE DERECHO
U.B.A.
IALAB