COLIN S. LEVY

Negotiating AI Terms

Negotiating AI Terms

Colin S. Levy

Legal disclaimer

This publication provides general information about contract issues involving artificial intelligence. It is not legal advice, does not address every law, regulation, industry, or jurisdiction, and does not create an attorney-client relationship.

Law and guidance change, and contract results depend on the facts. Readers should consult qualified counsel about their circumstances. The views expressed are the author's alone and do not necessarily reflect those of any employer, client, or affiliated organization.

Contents

Introduction

Begin by describing how the customer will use the service. An internal drafting assistant raises different issues from a system used for hiring, lending, health care, purchasing, payments, or changes to records. Before drafting, write down what the system does, who will use it, and which information it receives. Also identify whose rights, work, money, or access to a service may change, which decisions the system may influence, and whether it can act through another system.[1,6,10]

Review the deal in two stages. First, confirm the purpose, information, affected people, amount of automation, and reliance on other companies or services. Then address those facts in the contract, attached exhibits, testing requirements, and remedies. Record any unresolved assumptions. If the product design remains unclear or a key answer stays outside the signed agreement, revise the deal before approving it.

The agreement does not need every issue in this guide. Require basic protections before live use, then add terms when the service handles sensitive information, affects an important decision, or can take action. Assign each duty to the party that controls the relevant fact, system, or decision. State any customer action on which the vendor's performance depends.

How to use this guide

Lawyers will review these agreements with different experience and time available. The questions and review levels below show where to begin and how far to go.

- Newer reviewers should record the facts, choose a review level, and read the numbered sections listed for that level.
- Lawyers familiar with technology contracts can use the claim checklist, sample clauses, and examples to check the vendor's draft and refine their usual positions.
- If time is short, resolve the proposed use, information handling, authority to act, other providers, test results, remedies, and exit rights before live use.

A model is the part of a system that produces or evaluates a result. A prompt is a user's instruction or question. Output means what the service returns to a user or another system. Training or adjusting a model means using material to change how it later produces or evaluates results. An outside provider is a company that supplies a model, hosts the service, provides support, or handles information. An agent is a system that can use other programs or accounts to take actions. These descriptions explain how the terms are used here. A law may define them differently.

Record the key facts

Ask the business contact and vendor to answer these questions in writing. Record uncertainty instead of filling a gap with an assumption. The answers may appear in a request form, statement of work, product exhibit, security response, or another signed document.

Question	What to record
What will the service do?	List each function, result, process it supports, and affected system. Separate drafting, summarizing, recommending, deciding, and acting.
Who will use it or be affected?	Identify user groups, administrators, outside recipients, people affected by a decision, and the countries or states involved.
What information will enter or leave?	List public, confidential, personal, regulated, privileged, source code, login, and testing information.
Will it inform a person or take an action?	Identify recommendations, decisions, messages, payments, purchases, and record changes. State where approval occurs.
What can it reach?	List connected systems, sources, tools, and accounts. Separate permission to read, create, change, send, and delete.
Which other companies are involved?	Record outside models, hosting providers, support contractors, and other companies that receive customer information.
How will the customer judge success?	Name the task, test material, the current result without the service, the minimum acceptable result, and the consequence of failure.
Is this a test or live use?	State the dates, limits on information and users, testing rules, limits on relying on results, and who can approve live use.
What happens if it fails or disappears?	Describe delay to the business, legal exposure, financial loss, harm to a person, and any manual or other available process.
Who is responsible for each decision?	Identify the business contact responsible for the decision and the required legal, privacy, security, technology, purchasing, finance, and executive approvals.

Keep any unanswered question in the negotiation record. When a sales statement, demonstration, or security response affects the decision to buy or use the service, include the answer in the contract.

Choose a level of review

Use these levels as a starting point. They do not decide whether a law classifies the system as high-risk. Choose a more detailed review when facts remain unclear or an error could cause serious harm.

Level	Typical use	Terms to review
Focused	A limited test or internal tool uses public information or made-up test material that does not describe real people or business matters, does not make a decision with a significant effect, and cannot act through another system.	Service description, permitted use, limits on customer information, confidentiality, output rights, basic testing, notice of changes, fees, and deletion. Review sections 1, 2, 3, 5, 6, 8, 17, 19, and 20.
Expanded	The service receives confidential or personal information, produces work sent outside the organization, connects to an important system, or supports a process where an error could cause serious harm.	Everything in the Focused review, plus security records, limits on outside providers, testing before acceptance, records of important results, human review, responses to incidents, stronger remedies, and help moving to another service. Add sections 4 and 9 through 16.
Full	The use involves regulated information, decisions affecting a person's rights or opportunities, substantial legal or financial consequences, or authority to send, buy, pay, or change records.	Everything in the Expanded review, plus written limits on what the system may do, required approvals, tested safeguards, detailed records, clear assignment of legal duties, stronger protection from major losses, senior approval, and a tested alternative. Review every section, especially sections 7, 9, 10, 12, 15, 17, and 20.

How to choose: Review the most important provisions in greater depth. Those provisions concern sensitive information, decisions that affect people, changes to important records, movement of money, work sent outside the organization, and services that would be difficult to replace.

Review the deal in this order

Use this order so the parties define the service before they negotiate remedies and liability.

1. Confirm the intended use, users, information, connected systems, decisions, and permitted actions.
2. Choose a review level and identify the approvals required for it.
3. Request dated evidence before accepting claims about the product, security, performance, or insurance.
4. Put the service description, approved uses, information rules, outside providers, and steps the customer must take into signed documents.
5. Agree on testing, human review, limits on actions, records, responses to incidents, and how the parties will handle changes that affect the deal.
6. Match warranties, indemnities, liability limits, credits, termination rights, and other remedies to the agreed use.
7. Complete the agreed testing and confirm the product settings and safeguards before live use.
8. Review performance, product changes, incidents, pricing, and exit readiness during the term and before renewal.

1 Describe the service and its permitted use.

Define the covered service by what it does instead of relying on a broad definition of AI. Identify each model or service, its functions, connected systems, users, jurisdictions, and business processes. State whether it drafts, summarizes, recommends, decides, or acts. List prohibited uses and uses that require written approval. Put the description in a signed exhibit and require review of any AI function added later.[1,6,10]

The exhibit should list known limits, assumptions behind performance claims, steps the customer must take, and ways people may misuse the service. It should also distinguish testing from live use. A test may use limited information or made-up material that does not describe real people or business matters. The contract may also prohibit anyone from relying on test results. Those limits should change only when the customer approves live use in writing.

Review the vendor in light of how the customer plans to use the service. For an important use, examine the vendor's financial position, significant litigation, security reports, insurance, reliance on outside models, and ability to support the service. If another provider is essential, determine what happens if that provider changes its terms, raises its price, withdraws a model, or blocks the intended use.

2 List every type of information the service handles.

The words input and output do not cover every type of information. The agreement may need separate rules for customer files, prompts, personal or confidential information, output, records of use, and feedback. It may also need rules for information created from customer material, search records, sources consulted by the system, customer material used to adapt it, testing records, and account settings. For each type, state who owns it, who may access or use it, how long each party may keep it, and when each party must return or delete it.[1,6]

The vendor's license should cover only the uses needed to provide, secure, and support the service. The contract should require separate permission before the vendor uses customer material to train or improve a model, evaluate services for other customers, develop products, advertise, or disclose information to another party. If the customer permits the vendor to improve the service with customer material, identify the material covered, whether the permission is optional, how the customer may withdraw it, and what happens to material already collected. If the vendor may use information after removing identifying details, explain that process, prohibit attempts to identify people again, and limit combination with other information.

3 Separate rights in the service, customer material, and output.

The vendor may retain its models, software, and general methods without taking ownership of the customer's information, prompts, processes, or customer-specific work. Address any model adapted for the customer, collection of customer-provided reference material, connection to another system, template, or other item created during setup. Do not leave those items inside a broad definition of vendor technology.[1,2]

For output, obtain ownership of whatever rights the vendor can transfer and a broad, permanent license for the agreed use. In the United States, purely AI-generated material does not receive copyright protection, while human contributions may qualify case by case. State whether the vendor may keep or reuse output. Do not treat an ownership clause as a promise that the output is accurate, original, exclusive, or legally protected.[2]

4 Address the supplier's own use of AI.

A supplier may use AI to write code, provide support, analyze customer information, prepare advice, or create work for the customer even when the purchased product is not sold as an AI service. Require the supplier to explain whether and how it will use AI to perform the contract. List permitted uses in a signed exhibit. Before the supplier introduces a significant new use involving customer information, work provided to the customer, security, or legal compliance, require notice and written approval. Apply the same rule to contractors and subcontractors.[6]

If the supplier will not accept approval for every new use, limit the approval right to customer information and work that may carry serious consequences. Require notice and a right to turn off other new features. The supplier may then improve routine internal processes without approval if the change does not increase the customer's risk.

5 Require evidence for performance claims.

Put important claims from demonstrations, questionnaires, proposals, and sales presentations into the agreement or an attached exhibit. For each claim about accuracy, error rates, bias, speed, cost savings, or another measurable result, identify the tested version, date, method, sample, minimum result, and known causes of failure. Distinguish the vendor's testing from testing performed by the customer or an independent party.[1,7]

The FTC alleged that Workado marketed an AI content detector for general use even though its model had been trained or adjusted to classify academic material effectively. The final order requires competent and reliable evidence for future claims about accuracy or effectiveness and requires the company to keep that evidence.[7]

Where lawful and practical, test the service with customer material that reflects the work it will perform. Define who prepares the test, the minimum result, how many attempts the vendor gets, and what happens after failure. The contract should not treat the customer as accepting the service only because time passes. A vendor that will not guarantee every result may still promise that its statements are accurate in all important respects, its testing followed the stated method, the service meets the agreed written requirements, and the agreed safeguards work as described.

A test completed before signing may no longer apply after a change to the model, prompts, sources the system searches, or the process around it. For uses that could seriously affect a person or the business, require regular review and new testing after an important change. Define the required result, sample, notice, time to correct a problem, and right to stop the affected use if performance falls below the agreed level.[1,11]

6 State what happens when the service fails.

A service credit may be too little for a serious defect. Depending on the use, remedies may include correction, new testing, temporary use of an earlier version, a pause in the affected feature, repayment of prepaid fees, help moving to another service, or termination after repeated failure. State who must act and by when. Do not make a small credit the customer's only recovery for a serious failure.[1]

If service credits are the only remedy for failing to meet an agreed service level, state that limit clearly. Preserve separate rights for failures involving confidentiality, security, misuse of customer information, infringement claims, unauthorized actions, or termination rights stated elsewhere in the agreement.

7 Limit what an agent may do.

An agent is software that can work toward a task and act through connected tools rather than only producing text or information. If it can send messages, change records, initiate payments, purchase goods, or operate another system, put its permitted actions and limits in a signed exhibit. List the systems and tools it may access, the login information it may use, the information it may obtain, and the actions it may take. Set limits on money and transactions. Identify actions that always require human approval and actions that the system may never perform.[5,9]

- Show the proposed action and its important details before approval.
- Use the minimum access required for each task and separate read, create, change, send, and delete permissions.
- Require fresh approval if the amount, recipient, target, or another important detail changes after approval.
- Record the instruction, plan, action taken through a connected tool, approval, whether the action occurred, and the result.
- Allow an authorized person to pause, stop, and, where possible, reverse an action.
- Do not add a connection, tool, or category of action without the customer's approval.

The contract should state which party bears a loss when the system exceeds its agreed authority. The customer may remain responsible for approvals given by authorized users. The vendor should remain responsible when the service fails to enforce the agreed limits. The contract should not treat every automated act as the customer's act.

8 Match privacy and security terms to where information goes.

Identify where the vendor stores and handles each type of information, who can access it, which other companies receive it, and how long each party keeps it. Determine whether the service will receive personal information, regulated records, trade secrets, privileged material, source code, or login information. Require a current list of other companies that handle the information or supply a model on which the service relies.

The vendor should give notice before changing that list or another practice that affects the information and should address any serious risk created by the change. Add the terms that privacy law, health information law, rules on moving information across borders, and rules for the relevant industry require.[1,5,6]

The usual definition of a security incident may be too narrow. It may need to cover unauthorized use of customer information for training or improvement, exposure through another customer's result, and improper access by a connected tool. It may also need to cover changes to source material used by the system, disclosure of confidential system instructions, and an agent acting beyond its authority. State when the vendor must give notice, what facts the notice must include, which records each party must preserve, how the parties will cooperate, who must correct the problem, and who will notify affected people or regulators.

Set review rights according to the risk. Ask first for current independent audit reports, test summaries, and recognized certifications. If those materials do not address the product version, planned use, or information involved, allow follow-up questions, supporting records, and an independent review. Set practical limits on notice, frequency, confidentiality, what the review may cover, and cost without making the right unusable.[1,11]

If the service will receive information relating to a legal representation, review the vendor's terms, privacy policy, who can access the information, training practices, and security safeguards against the professional duties that apply. The lawyer must still assess competence, confidentiality, supervision, and any consent required for the intended use.[12]

9 Keep records that explain an important result.

Require records detailed enough to show what happened. For important uses, record the model and version, instructions and settings that affected the result, sources consulted, actions taken through connected tools, approvals, dates and times, output, and later corrections. Give the customer access in a usable format and set a period for keeping the records that fits legal, regulatory, and dispute needs.[1,3,5]

NIST's voluntary Generative AI Profile recommends records of testing, versions, changes, and incidents. The EU AI Act requires providers and deployers of covered high-risk systems to keep automatically generated system records, which the Act calls logs, under their control for at least six months unless another law provides otherwise. Under the current consolidated text, the relevant Chapter III requirements generally begin on December 2, 2027 for high-risk uses listed in Annex III and on August 2, 2028 for high-risk systems built into regulated products covered by Annex I. If the agreement will remain in force then, address access to those records now.[1,3]

The records should not collect sensitive information that the parties do not need. Limit each record to needed information, restrict access, protect the records from changes, and keep them only as long as legal, business, and dispute needs require.[1,11]

10 Assign legal duties and required help.

A general promise to follow applicable law is not enough. Identify each party's role under the laws that apply. The EU AI Act uses the terms provider and deployer. Privacy laws may use controller and processor. Workplace laws may place duties on an employer. Assign responsibility for notices, assessments, testing, records, human review, complaints, responses to regulators, and corrections. Require each party to supply the information the other reasonably needs to perform its duties.[3,10]

For a high-risk system, the EU AI Act can treat a distributor, importer, deployer, or other outside party as the provider in three situations. The rule applies when that party places its name or trademark on the system, makes a substantial modification while the system remains high-risk, or changes the intended purpose so that a previously lower-risk system becomes high-risk. State which customer settings and connections to other systems remain within the vendor's approved design. Require advance warning if a requested change could alter either party's legal role. The vendor should then provide the documents, access needed for testing, known limits, and other help needed to comply with the law. The contract may divide the work and cost, but it cannot remove a duty imposed by law.[3]

11 Assign notices, labels, and ways to question a result.

State who must tell a person that the service uses AI, label generated or altered material, preserve source information, and provide a way to question or correct a result. The vendor should supply working features and accurate instructions. The customer should provide the notices and review process required for its use.[3,4]

Article 50 of the EU AI Act has applied since August 2, 2026. It requires notice when people interact directly with certain AI systems and requires some generated or altered content to carry a mark that software can detect. Organizations using the systems must also make disclosures for certain uses. A limited grace period applies to the marking duty in Article 50(2) for systems placed on the market before August 2, 2026; providers of those systems must comply by December 2, 2026. Check the rule and its exceptions for the service at issue because the duties do not apply to every AI interaction or output.[3,4]

12 Define how human review will work.

The contract should give the reviewer enough information, time, authority, and access to intervene in the system. When the use requires it, the system should show the basis for a result and its known limits. Reviewers should be able to disregard, correct, stop, or reverse the result. For decisions affecting individuals, determine whether the person needs notice, an explanation, a way to challenge the result, or an alternative that does not depend only on automation.[3,5,9]

Provide training and support for reviewers. The vendor should explain the system's functions and known limits. The customer should choose qualified reviewers, set internal procedures, and make sure routine approval does not become automatic.

Name the decisions that require review and the point at which review must occur. Once the system sends a message, changes a record, or releases a payment, later approval cannot change that action. Give the reviewer enough time and information to make an independent decision.[5,9,12]

13 State warranties the vendor can honor.

A vendor may reasonably refuse to promise that every AI result will be correct. That refusal does not justify providing the service "as is" or disclaiming the promises elsewhere in the agreement. Require the vendor to promise that it has the rights needed to provide the service and follows its stated testing method. It should also meet the agreed documentation and written requirements, comply with the laws that apply to its part of the service, use customer information only as permitted, and keep the agreed safeguards working.[1,6,7]

If the vendor refuses a broad performance warranty, limit the promise to the named use, defined test conditions, and disclosed version. Preserve remedies when the vendor concealed a known limit, misstated a test, or allowed an agreed safeguard to fail. State that general disclaimers do not override the express warranties, limits on information use, security terms, or indemnities elsewhere in the agreement.

14 Draft indemnity language for the claims that may arise.

An indemnity limited to infringement by software may not cover claims involving information used to train or adapt a model, generated content, recommendations, or automated actions. State what the indemnity covers. Review exclusions for combinations, modifications, customer material, and commercial use. Apply an exclusion only when the excluded conduct caused the claim.[2]

Review the customer's indemnity as closely as the vendor's. Language covering every claim arising from the customer's use can make the customer responsible for a claim caused by the vendor's system. Limit the customer's indemnity to its breach, unlawful material, prohibited use, or other conduct within its control. Address who controls the defense, settlements that restrict continued use, replacement or modification of the service, and repayment if no practical fix exists.

15 Set liability limits for the planned use.

A liability limit based on a short period of fees may bear little relation to a privacy event, infringement claim, failure to meet a legal duty, unauthorized automated action, or failure in an important business process. Consider a higher limit for claims covered by the intellectual property indemnity, breaches of confidentiality, privacy or security failures, unauthorized use of customer information, and duties central to the planned use. Address fraud, gross negligence, willful misconduct, and any other exceptions required by the governing law or recognized elsewhere in the agreement.

Do not create a separate liability limit for "AI-related loss" unless the agreement defines that term. If the vendor will not accept a higher limit for every failure, identify the events that could cause the most serious and foreseeable harm. Apply the higher limit to named duties or events.

16 Keep a current list of outside services and components.

List the important models, connections to other services, add-ons, open-source components, hosting providers, and tools on which the service depends. For each one, record its function, access to customer information, license terms, and replacement process. Require an update when an important item changes. NIST's voluntary guidance recommends keeping a list of outside AI and software components, reviewing them, and testing backup options.[1,5]

A vendor may need to replace an outside model. Permit a replacement if it does not significantly worsen agreed performance, information handling, legal status, security, ability to work with other systems, or cost. Require testing and notice in advance. If the customer reasonably rejects an important change, allow use of the prior version for enough time to switch or permit termination with repayment of unused prepaid fees.

17 Limit changes the vendor may make on its own.

Identify every web page and policy that forms part of the agreement. State which document controls if terms conflict. Prevent an online policy from overriding a negotiated term. Require notice before a change to the model, function, supported use, information handling, security safeguard, outside service, or price. Give the customer time to test the change and a remedy if it causes serious harm.[1,6,10]

The agreement should separate ordinary maintenance from a change that alters performance, legal classification, or customer duties. The vendor may control routine maintenance, while the customer receives testing, objection, or termination rights for more important changes. If a change in law makes the agreed use unlawful or significantly more costly, require prompt notice and a reasonable plan to address it. Allow the customer to end the service and recover unused prepaid fees if no lawful solution is available.

18 Limit suspension rights.

Vendors need to stop activity that presents an immediate security, legal, or safety threat. They should not have an unlimited right to suspend an entire account based on an unexplained suspicion. Require a factual basis and notice unless immediate action is necessary. Limit the suspension to the affected user or function, name a person who can review the decision quickly, and require service to resume within a stated period after the parties resolve the issue.[1]

After an emergency suspension, require a written explanation and the information reasonably needed to prevent the problem from happening again. Preserve access to unaffected information and services. NIST's voluntary profile recommends reviewing vendor contracts for arbitrary termination of important generative AI services and stating how quickly the vendor must respond to incidents and provide support.[1]

19 Explain how use creates charges.

Pricing based on use needs more detail than a rate. Define whether charges cover prompts, output, stored or reused material, calls to other tools, automated steps, searches, storage, failed requests, or repeated attempts. State how the customer can verify use. Require current usage and billing records, alerts, spending limits, and approval before charges exceed an agreed amount. Set a period for disputing charges and preserve the records needed to resolve the dispute.[8]

Address unused commitments, whether unused amounts carry forward, limits on use, price changes, and any different rate after a model replacement. Avoid an inflexible minimum commitment when use remains uncertain. If the vendor requires one, negotiate a lower starting amount, increases tied to actual use, a limited right to carry unused amounts forward, and termination or price protection after an important change. In an inquiry about cloud competition, some commenters told the FTC that minimum-spend contracts, fees for moving information, and cloud credits could make switching harder. Review those terms closely when an AI service depends on cloud services and similar pricing methods.[8]

20 Agree on export, deletion, and help moving to another service.

Require export of customer information, prompts, output, system records, account settings, collections of customer-provided reference material, and other agreed material in a documented and usable format. Set the time, price, and method for export. Require deletion from active systems and backups according to a stated schedule, followed by written confirmation. Address continued rights in output and work already created.[1,9]

For an important service, require help moving to another service and a tested backup process. The backup may use another provider, an earlier model, a limited internal system, or manual work. Address insolvency, loss of an outside provider, an unlawful location for handling information, a prolonged outage, and an important product change. Export rights alone may not preserve a business process if the customer cannot export settings, source links, stored history, preferences, or other material needed to reproduce the service. Test the export and backup process before live use or early in the term.

21 Check whether insurance covers likely claims.

Require appropriate technology errors and omissions insurance, cyber insurance, and, when relevant, media liability insurance. Review exclusions for automated decisions, generated material, intellectual property claims, unauthorized actions, and regulatory investigations. Match the request to the planned use. Begin with a certificate and written answers about relevant exclusions. For an important use, request the policy declarations and any endorsement that changes coverage, confirmation from the broker or insurer, or another focused form of evidence. A certificate lists coverage and limits but does not establish that the policy covers a particular claim.[15]

22 Set negotiation priorities before revising the contract.

Decide which terms the customer requires before live use, which depend on the planned use, and which can change during negotiation. Assign each duty to the party that controls the relevant fact, system, or decision. The customer controls its users, approved information, and final business decisions. The vendor controls its service, product statements, outside components, security measures, and product changes.[1,6,10]

- Before revising the legal terms, resolve the intended use, what the service includes and excludes, the users, the information, and the actions the system may take.
- Ask for evidence early. If the vendor cannot explain its test method, the outside services on which the product relies, or where information goes, limit the proposed use or pause the review until it can.
- Put answers that affect approval into signed exhibits or contract promises.
- For each issue that could change approval, record the reason, evidence received, first request, narrower option, and decision maker.

- Record the limit on each concession. For example, exclude sensitive information from training, require equivalent testing for a replacement model, or require prompt review after an emergency suspension.

23 Include customer-specific AI artifacts in data, export, and deletion terms.

Do not limit customer information to files uploaded directly to the service. An AI service may create prompts, output, embeddings, vector representations, indexes, retrieved collections, caches, logs, saved workflows, customer-specific settings, and models adapted for the customer. Identify which of these items the service creates and state which party may access, use, retain, export, or delete each one. A change in technical form should not remove an agreed restriction on customer information.

Define customer information broadly enough to cover material supplied by or for the customer and representations derived from that material. Preserve the vendor's ownership of its general service, models, software, and methods without allowing that definition to absorb customer-specific work. For each relevant artifact, address:

- where it is stored and which companies can reach it;
- whether it may be used for training, improvement, testing, or another customer;
- whether the customer can export it in a documented and usable form;
- how long it remains in active systems and backups; and
- what evidence will confirm return or deletion.

If the vendor adapts a model for the customer, determine whether the customer needs the model itself or whether configuration files, instructions, evaluation sets, source links, and other materials will allow a replacement service to reproduce the work. The vendor should disclose any technical limit on export or deletion before using customer information for adaptation. The agreement should then set the permitted use, retention period, and remedy if the vendor cannot perform the promised return or deletion.

> For a service within the EU Data Act's rules for data processing services, the statutory definition of exportable data includes customer input and output data and related metadata, subject to stated exclusions. The contract should identify the covered categories and may provide broader rights where the statutory definition does not capture every customer-specific artifact.[13]

24 Add DPA and privilege terms when the information requires them.

When the service handles personal information and applicable law requires processor terms, use a data processing agreement that matches the actual AI service. A standard form may omit training, model providers, connected tools, derived representations, and product changes. Map each processing activity before assigning controller, processor, or other legal roles. The title of the document matters less than whether the terms describe the real information flow.

The DPA or equivalent terms should address:

- the purpose, duration, locations, information types, and people involved in each processing activity;
- documented instructions and any prohibited use for training, improvement, benchmarking, or another customer;
- a current list of subprocessors and model providers, advance notice of changes, an objection process, and written duties that follow the information downstream;
- security measures, incident notice, audit evidence, and help with individual rights, assessments, investigations, and regulator requests; and
- return and deletion of prompts, output, logs, embeddings, vector representations, indexes, caches, customer-specific settings, and backups according to a stated schedule.

Information relating to a legal representation requires a separate privilege and confidentiality review. Confirm who can see the material, whether people use it for support or review, whether any model or outside provider retains it, how the vendor responds to legal process, and whether the service can isolate matters and users. Limit the information supplied to what the task requires. Determine whether the client must be told about the use or provide informed consent under the professional rules that apply.[11,12]

> A contract can support confidentiality, but it cannot guarantee that a court or regulator will treat a communication as privileged. Record the legal and factual basis for the decision to use the service, the safeguards reviewed, and any client instruction or consent.

25 Identify current regulatory duties before signing.

Identify the places, people, decisions, and industries connected to the planned use before naming laws in the agreement. The same service may fall outside a rule for one customer and within it for another. State which party will determine classification, provide supporting information, keep required records, give notices, complete assessments, respond to individuals and regulators, and correct a failure. Require notice when a product or legal change may alter that allocation.

The EU Data Act has applied since September 12, 2025. When its switching rules cover the service, the contract must address the categories of exportable data and digital assets, switching assistance, service continuity, known technical limits, a maximum notice period of two months, and ordinarily a maximum transitional period of 30 calendar days. It must also provide at least 30 calendar days for retrieval after the transition and address erasure after that period or a later agreed date. A provider may use a longer transition, up to seven months, only when it gives timely notice and justifies technical infeasibility. Confirm that the particular service falls within the Act before relying on these rights.[13]

Colorado replaced its earlier AI statute in 2026 with the Automated Decision-Making Technology Act, effective January 1, 2027. The law covers specified technology used to materially influence consequential decisions. Among other duties, it requires developers to provide technical documentation about intended uses, categories of training data, known limits, appropriate use, and human review, and to notify deployers of material updates. Deployers have notice, correction, human-review, and other duties for covered decisions. Developers and deployers must retain records needed to show compliance for at least three years. Rulemaking was still underway as of September 5, 2026, so the contract should require updated information and cooperation instead of freezing incomplete regulatory details.[14]

> Also check the laws governing the activity itself, including privacy, employment, lending, health information, insurance, education, professional duties, and consumer protection. Do not assume that a general promise to follow applicable law supplies the documents, product features, or assistance the customer needs. Name those deliverables and connect each one to a deadline and remedy.

Check the vendor's claims

Ask for dated evidence because a vendor's answer may describe an older version or a different product. The records should identify the system, version, date, method, and what the review covered. A confidentiality agreement, secure review room, summary, or independent report can protect sensitive vendor information while giving the customer enough information to review the claim.

Vendor statement	Evidence to request
We do not use customer information to train our models.	A written description of where customer information goes; the product, privacy, and deletion terms; and the terms that bind each outside model provider.
The service is accurate.	A dated report naming the version, task, sample, method, result, causes of failure, and similarity to the customer's work.
We delete customer information.	The deletion schedule for active systems and backups, exceptions, method, outside-provider duties, and written confirmation.
A person approves important actions.	Product instructions, a test of the approval feature, a sample record, and proof that a changed action requires new approval.
The service is secure.	Current independent reports and test summaries, access restrictions, incident procedures, and coverage of connected tools and outside models.
Our outside providers meet the same standards.	A current list with each provider's role and access, written confirmation of its contract duties, and the rules for notice and objection.
Customers can use the output safely.	Available sources and origin details, known limits, tests for the planned use, excluded uses, and the response to infringement or harmful output.
The customer can switch providers easily.	A sample export, file description, timing, cost, included settings and records, deletion steps, switching help, and a recent export or backup test.

How to review it: Compare the evidence with the draft contract, online policies made part of it, security exhibit, and order form. Ask the people responsible for the product, privacy, and security to explain any inconsistency before deciding whether contract language can resolve it.

Use these sample clauses

These examples turn a business requirement into contract language. Adjust them to match the contract's definitions, the product, governing law, bargaining power, and other transaction documents. Brackets mark a choice that must be made for the deal. These examples mostly state the customer's position. Vendor counsel can use the same issues to identify what the product can do and where the facts justify a narrower term.

Customer information Allow the vendor to use customer information to provide the service. Require separate permission for any broader use.

> **Starting point:** Vendor may use Customer Information only to provide, secure, maintain, and support the Service for Customer. Vendor will not use Customer Information to train, adjust, test, or improve a model or service for Vendor or another customer without Customer's express written consent identifying the information and permitted use. Vendor will impose the same restrictions on each outside provider.

Narrower option: Limit permission to improve the service to identified, non-sensitive information; prohibit use by an outside model provider; allow withdrawal for future use; and set a deletion rule.

Place it in: *The AI exhibit, terms governing the handling of information, and the clause stating which document controls.*

Output rights State what the customer may do with output without assuming that every output receives copyright protection.

> **Starting point:** Customer retains all rights in Customer Information. Vendor assigns to Customer any transferable right Vendor may have in Output. If Vendor retains a right in Output or cannot effectively assign it, Vendor grants Customer a perpetual, worldwide, transferable, sublicensable, royalty-free right to use, reproduce, modify, distribute, display, perform, and create derivative works from Output for any lawful purpose. Vendor will not reuse Customer-specific Output except to provide the Service to Customer.

Narrower option: Retain customer ownership of information it provides and customer-specific work, obtain a permanent license to output, and prohibit reuse that exposes confidential information or identifies the customer.

Place it in: *Intellectual property terms and the AI exhibit.*

Performance and acceptance Base the warranty on a defined task and test. Do not make it apply to every possible result.

> **Starting point:** Vendor represents that the documentation and test results supplied to Customer are accurate in all material respects for the identified version and stated test conditions. Customer will test the Service under the acceptance procedure in Exhibit [X]. If the Service does not meet an agreed measure, Vendor will correct and retest it within [period]. After [number] failed attempts, Customer may reject the affected function, recover prepaid fees for it, or terminate the affected order without penalty.

Narrower option: Require accurate statements, compliance with documentation, working safeguards, time to correct a failure, and a right to stop using a failed feature even if the vendor will not guarantee every output.

Place it in: *The product schedule, acceptance exhibit, warranties, and remedies.*

Outside providers and model changes Set conditions for replacing an important model or provider.

> **Starting point:** Vendor remains responsible for each outside provider used to perform the Service. Vendor will notify Customer at least [30] days before changing an important model or outside provider when the change may affect performance, information handling, security, legal compliance, compatibility with other systems, or price. The change will not materially reduce the agreed protection or function. If Customer reasonably objects, the parties will pursue a practical alternative. If none is available, Customer may stop the affected use or terminate it and receive a refund of unused prepaid fees.

Narrower option: Require notice, the same limits on information use, defined limits on reduced performance or security, and a right to disable the feature or end the service after a change that materially reduces either one.

Place it in: *Terms governing subcontractors, the AI exhibit, product changes, and termination.*

Authority to act Use this only when the service can act through another system.

> **Starting point:** The Service will not take an External Action except as permitted by the Authority Schedule. It will display the proposed action and its important terms before any required approval, enforce the stated access and transaction limits, and obtain a new approval if an important term changes. Vendor will keep a record of the instruction, approval, action, and result and will provide a feature that allows an authorized user to stop the affected function promptly.

Narrower option: Limit the service to drafts or recommendations, remove permission to change records, require approval in the connected system, and set low transaction limits until the safeguards pass testing.

Place it in: *The authority schedule, security exhibit, acceptance test, and liability terms.*

Suspension Allow suspension for a real emergency and limit its reach and duration.

> **Starting point:** Vendor may suspend only the user, connection, function, or activity reasonably necessary to address an immediate and material security, legal, or safety threat or an uncured material breach. Vendor will give prior notice unless delay would materially increase the threat, provide a contact for prompt review, preserve access to unaffected information and functions, review the suspension promptly, and restore service when the reason has been resolved. Vendor will provide a written explanation after an emergency suspension.

Narrower option: At minimum, limit the suspension, require prompt notice and a contact for quick review, preserve access to information that can be exported, and require the vendor to resume service after the cause ends.

Place it in: *The suspension clause, service levels, support terms, and plan for a service interruption.*

Disclaimers and express promises State that a general disclaimer does not override negotiated promises.

> **Starting point:** No disclaimer concerning output or use of artificial intelligence overrides Vendor's express warranties, restrictions on information use, confidentiality and security duties, indemnities, agreed performance measures, or obligation to enforce the safeguards described in the Agreement. No disclaimer limits a remedy for Vendor's material misstatement, unauthorized use of Customer Information, or failure to provide an agreed safeguard.

Narrower option: List the specific provisions that the disclaimer does not override and preserve correction, suspension, refund, and termination rights for failures the vendor controls.

Place it in: *The warranty disclaimer and the clause stating which document controls.*

Exit and deletion State what the vendor must return, when it must return it, and what it may charge before the customer depends on the service.

> **Starting point:** During the term and for [period] after termination, Vendor will provide Customer Information, Output, agreed records, settings, and collections of Customer-provided reference material in the documented formats listed in Exhibit [X]. Vendor will complete the export within [period] at the charges stated in the Order Form, provide the agreed help moving to another service, and delete Customer Information from active systems and backups under the deletion schedule. Vendor will confirm completion in writing and may keep information only as an identified law requires.

Narrower option: Require a standard export at no added charge, a fixed price for additional help, continued access while the customer moves to another service, and written confirmation of deletion.

Place it in: *Termination, return of information, help moving to another service, and the order form.*

Adjust the review to the planned use

A clause may matter more in one transaction than another. These examples identify the issues that deserve the closest review for four common uses.

An existing software provider adds an AI feature. Check whether the feature is on by default, which information it receives, whether current limits and indemnities cover it, and whether an online policy changes the contract. Focus on the right to turn the feature off, information use, model replacements, price changes, and the effect on existing processes.

A standalone tool drafts, summarizes, or reviews legal work. Examine confidentiality, privilege, deletion, model training, information about sources, output rights, performance testing, and user review. Determine whether the tool stores matters separately and whether administrators or support staff can see the material.

A supplier uses AI while performing services. Ask which tasks involve AI, what customer material enters another service, who reviews the work, and who owns the work delivered. Keep the supplier responsible for its work, confidentiality, outside providers, and errors. The supplier should not use AI as a reason to shift all review to the customer.

A system can send, buy, pay, or change records. Review the system's authority separately. Use a signed list of permitted actions, limited login information, approval rules, low initial limits, action records, and ways to stop the system in an emergency. Test the limits before acceptance and state who bears a loss when the service fails to enforce them.

A narrower review may be reasonable when the tool uses only public information or made-up test material that does not describe real people or business matters. It should not create work for people outside the organization, affect a decision with serious consequences, or take action. It should remain easy to disable and stay within a short, controlled test. Record those limits and require another review before the use expands.

Check the service before live use

Before the service goes live, confirm that the product settings, internal procedures, and user instructions reflect the agreed limits.

- The signed documents identify the approved functions, users, information, systems, jurisdictions, and prohibited uses.
- The customer has dated copies of each online policy made part of the contract, and the contract states which document controls if terms conflict.
- The configured product uses only approved outside models, connections, locations, periods for keeping information, and information settings.
- User permissions separate reading, creating, changing, sending, and deleting where the product supports those distinctions.
- The acceptance test used appropriate material, recorded the version and settings, met the agreed result, and documented known limits.
- Required human reviewers understand the task, limits, timing, person to contact with a problem, and authority to reject or stop a result.
- Any system that can act has passed tests of approval, changed terms, access limits, transaction limits, records, and emergency stopping.
- Legal, privacy, security, technology, purchasing, finance, and business approvals required by the chosen review level are complete.
- Contacts for incidents, notice procedures, support response times, correction periods, and contacts for quick review of a suspension are current.
- Usage records, alerts, spending limits, invoice records, and approvals for charges above the agreed amount are working.
- The customer can obtain the agreed system records, sources, settings, output, and other material needed to review an important result.
- The customer has completed a sample export and confirmed that a manual or other process can support a serious interruption.

Before renewal: Review the changes made during the term.

- Compare the current model, outside providers, places where information goes, functions, and online policies with the signed description of the service.

- Review performance results, incidents, complaints, decisions that people reversed, unauthorized actions, and fixes that remain incomplete.
- Confirm that legal roles, notices, records, human review, and required assessments still fit the actual use.
- Ask for more security and insurance evidence when the service can cause greater harm or handles more sensitive information.
- Review use, pricing, commitments, the ability to export, and the cost of switching before accepting the renewal term.

Keep one record of the negotiation

A short, current record helps lawyers with different levels of experience work from the same facts. Keep one row for each important issue and link it to the supporting records and final document. The record can sit in a spreadsheet, contract system, or matter file.

Field	What to record
Issue	State the specific question or contract requirement. Avoid a broad label such as AI risk.
Reason	Explain why the use, information, person, system, cost, or legal duty makes the issue important.
Evidence	List what the vendor supplied, its date and version, and any unanswered point.
First request	Record the language or practical result first requested.
Narrower option	State the narrower term, product safeguard, limit during testing, price adjustment, or exit right that would remain acceptable.
Stop condition	Identify the fact or refusal that prevents the proposed use from proceeding.
Decision maker	Name the person authorized to accept an exception and the date of the decision.
Final location	Cite the section, exhibit, policy version, record of the product setting, or internal procedure that contains the result.
Next action	State what must happen before live use, during use, at renewal, or at exit, and assign a person and date.

The final contract documents should let a new reader understand the approved use, negotiated protections, accepted exceptions, and work that remains after signing without relying on memory or an email search.

Endnotes

1. National Institute of Standards and Technology, Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile, NIST AI 600-1. Accessed September 5, 2026.
2. U.S. Copyright Office, Copyright and Artificial Intelligence, Part 2: Copyrightability. Accessed September 5, 2026.
3. EUR-Lex, consolidated text of Regulation (EU) 2024/1689 as of July 27, 2026. Accessed September 5, 2026.
4. European Commission, Transparency Obligations Under Article 50 of the AI Act: Questions and Answers. Accessed September 5, 2026.
5. OWASP, AI Agent Security Cheat Sheet. Accessed September 5, 2026.
6. Victorian Government, Navigating AI in Procurement. Accessed September 5, 2026.
7. Federal Trade Commission, Final Order Against Workado Concerning AI Accuracy Claims. Accessed September 5, 2026.
8. Federal Trade Commission, Cloud Computing RFI: What We Heard and Learned. Accessed September 5, 2026.
9. UK Competition and Markets Authority, Agentic AI and Consumers. Accessed September 5, 2026.
10. European Commission Public Buyers Community, Updated EU AI Model Contractual Clauses. Accessed September 5, 2026.
11. UK Information Commissioner's Office, Contracts and Third Parties: Artificial Intelligence. The ICO states that this guidance is under review following changes made by the Data (Use and Access) Act. Accessed September 5, 2026.
12. American Bar Association Standing Committee on Ethics and Professional Responsibility, Formal Opinion 512: Generative Artificial Intelligence Tools. Accessed September 5, 2026.
13. EUR-Lex, Regulation (EU) 2023/2854 on harmonised rules on fair access to and use of data (Data Act). Accessed September 5, 2026.
14. Colorado General Assembly, Senate Bill 26-189: Automated Decision-Making Technology. Accessed September 5, 2026.
15. New York State Department of Financial Services, Certificates of Insurance. Accessed September 5, 2026.

About the author

Colin S. Levy is General Counsel at Malbek and an Adjunct Professor at Albany Law School, where he teaches technology and law practice management. He has spent more than a decade as an in-house lawyer at technology companies.

He is the author of The Legal Tech Ecosystem and the forthcoming Code Switched: A Lawyer's Guide to the Era of AI, co-author of CLM for Dummies, and editor of the Handbook of Legal Tech. He serves on the board of the Corporate Legal Operations Consortium, advises legal technology companies, and writes and speaks about artificial intelligence, contracts, how legal teams work, and the practical use of technology in law.

Levy earned his J.D. from Boston College Law School, a B.A. with honors from Trinity College, and a certificate in legal innovation and technology from Suffolk University Law School.

colinslevy.com