SOLVING LEGAL · CLIENT DOSSIER

Your matter and artificial intelligence

How the firm works with artificial intelligence, and why your information is protected

INTRODUCTION

This dossier brings together in a single document the sections that answer the questions a client rightly asks on learning that the firm handling their matter works with artificial intelligence. It applies equally to a private individual and to a company, and it explains the how, never the what of any specific case.

Three things worth being clear about from the outset

- Artificial intelligence does not decide your case or replace your lawyer. It proposes; the lawyer verifies, resolves and is accountable for the work.
- Your information does not leave the firm; it is handled in a professional environment with a contract and safeguards, and the most sensitive material does not even enter the tool.
- Nothing is filed or sent on its own. What the tool produces is a working draft; anything that goes out is decided and signed by your lawyer.

Contents

SECTION 01

What it means for your lawyer to use artificial intelligence in your matter

Learning that the firm handling your case works with artificial intelligence understandably prompts two reactions at once: it sounds like an advantage and a cause for unease in equal measure. It is worth setting things straight from the start. What the firm has adopted is not a robot that replaces the lawyer's judgement, but a disciplined way of using a tool precisely where it genuinely helps, with your lawyer deciding and remaining accountable throughout.

1.1 A tool, not a replacement

Artificial intelligence is used here for what it does well: reading large volumes quickly, organising documentation, locating what is relevant within a voluminous file and preparing working drafts. It is not used for what it should not do, namely deciding the strategy of your case or accepting a conclusion as sound without a lawyer checking it. The rule that governs everything else is simple and admits no exception: the tool proposes; the lawyer verifies and decides.

1.2 What changes for you, and what does not

For you, two things change above all, both in your favour. The mechanical work that used to take up hours — reviewing bundles, cross-checking dates, searching for precedents — is done in less time, and the lawyer spends that freed-up time on what calls for judgement. On top of that, the analysis comes with a safety net: the method requires citations to be checked and does not allow anything to be settled while it still turns on facts not yet on record (this is developed in the section "Why it does not lower the quality of your defence").

What is essential does not change. You still have a lawyer who knows your matter, who attends to you and who is accountable for their work. Artificial intelligence does not deal with you or speak on the firm's behalf: it is an internal instrument, no different in kind from a legal database or a word processor. With one difference that justifies every precaution: when it gets something wrong, the mistake comes disguised as a right answer.

1.3 Why the firm tells you this

A firm could use these tools and say nothing: nothing obliges it to spell out the methods it works with behind the scenes. If it is explained here, it is for two reasons. The first is trust: better that you should know how your information is handled than find out by chance. The second is consistency: a system whose whole point is to leave a trace of everything it does would sit oddly with hiding that it exists at all.

SECTION 02

Your confidentiality and your data

When a firm brings artificial intelligence into its work, a client's first legitimate question is not whether the tool is clever, but whether their matter remains theirs. It is the right question: there would be little point in a sharper analysis if the price of it were any loosening of the duty of secrecy a lawyer owes to those who place their trust in them. It is worth saying plainly before going into detail. Here, artificial intelligence is used with real data only in a way that can be explained and defended before anyone who asks: the client themselves, a supervisory authority or a court.

2.1 The firm does not relinquish control over your information

The firm is and remains the controller of your data: artificial intelligence works as a tool under its control, not as a third party that keeps your information or decides for itself what to do with it. The difference is easiest to see in reverse. When someone pastes a file into a general-purpose chatbot, the data leaves the firm's hands at that very instant, passing to a service that may retain it, reuse it or use it to train its models, with no record of where it went and no way to get it back. That does not happen here: the material never leaves the professional environment within which the firm remains accountable for it.

2.2 What protects your material specifically

- **Data perimeter.** Your material is only handled within a professional environment that includes a data processing agreement (art. 28 of the GDPR) and a commitment not to use your data to train the models; never on personal or free-of-charge plans, where those safeguards simply do not exist.
- **Your matter is not mixed with any other.** Your information lives within the firm's own environment, with no central server pooling the data of several clients or several firms: that pooling is precisely what multiplies the risk of one matter bleeding into another or leaking out.
- **The most sensitive material does not even enter.** Anything that by its very nature must not leave the firm — proceedings under a formally declared secrecy order, or matters whose disclosure would in itself be a criminal offence — is not handled with artificial intelligence at all, but kept separately, in encrypted storage outside the cloud.
- **Nothing is taken as sound on its own.** No output is accepted or acted on without your lawyer reviewing and authorising it: the system does not send, file or publish anything of its own accord.
- **A trace remains of every step.** The firm keeps its record of processing activities (art. 30 of the GDPR), its security measures in writing and a history of each action; if an account ever has to be given, it can be.

2.3 Why this is defensible

The key lies in what the law actually requires. The GDPR does not demand zero risk — which exists in no data processing, whether involving artificial intelligence or not — but rather being able to demonstrate the diligence with which the work is done: this is the accountability principle of art. 5.2. For you, this means that diligence here is not merely asserted but evidenced: the system records each step as it goes, rather than ticking a box once and forgetting it. Exactly what exists to be shown — to you, to a supervisory authority or to your own auditor — is set out in the section "If you are audited".

SECTION 03

Why it does not lower the quality of your defence

The most reasonable misgiving about artificial intelligence in law is not that it is clumsy, but the opposite: it writes so well that it is hard to tell when it is right from when it is wrong. A general-purpose tool delivers a doubtful answer in the same confident tone as a sound one, with no warning sign, and the error slips past the guard of anyone in a hurry or too inclined to trust it. In your matter, that would translate into three specific risks; against each one, the method puts up a defence.

3.1 Citations that do not exist

The best-known failing: the tool cites made-up judgments, or attributes to an article something the article does not say, with a reference that has a court, a date and a number and that passes for genuine until someone looks it up and finds nothing. Here no citation is taken as true simply for appearing in the answer; every reference to a rule or to a ruling is checked against the official source before anything is built on it. What cannot be verified is flagged and stopped, rather than dressed up as a conclusion.

3.2 Out-of-date law

Nor does the tool know the reforms that came after the point at which it was trained, and it may apply the wording of a rule that has already changed without warning of it. The method starts from the opposite premise: the rule governing your matter is the one in force on the date of the events, not today's version, so the wording as at that date is consulted and any later changes are flagged. And there is a safeguard for you in this too: a later, more lenient reform may work in your favour, and it is worth not letting it slip by.

3.3 Conclusions wrongly closed off

The third risk is subtler: the tool tends to close off what should stay open, asserting a time limit, a legal characterisation or a conclusion that in truth turns on facts in the file it does not have before it. When a fact is missing, the method does not paper over the gap with a guess; it marks the point as pending and refers it to the lawyer. Caution is written into the procedure, not entrusted to anyone's good memory.

3.4 What you gain

The upshot: your matter is less exposed to an error wearing the mask of certainty, and the analysis reaches the lawyer's desk already filtered. Far from diluting their judgement, it sharpens it, because the tool takes the mechanical work off their hands and gives the case back refined for what really matters — deciding. It is a complement to the lawyer's judgement, never a substitute for it.

SECTION 04

Who decides and who is accountable

When a client knows that artificial intelligence is involved, one question always lingers: who is really in charge of their case. The answer is clear and worth giving plainly, because everything else depends on it holding up.

4.1 The tool proposes, the lawyer disposes

Artificial intelligence proposes and marshals the work, but it does not choose the strategy of your matter, it does not weigh the evidence and it does not exercise legal judgement. The last word always rests with your lawyer: they are the one who reads what the tool prepares, tests it and decides what to do with it. The tool does not sign pleadings, it does not appear in the proceedings and it does not share in the accountability; that accountability rests entirely with the lawyer, just as it did when everything was drafted by hand.

4.2 Nothing leaves the firm of its own accord

That boundary is not held up by a statement of intent, but by a material rule that the system observes by design: it does not send, file or publish anything by itself. Everything that goes out — from a pleading that is filed to an email that is sent — is a manual, deliberate act by the lawyer; nothing leaves the firm unless a person has chosen to send it. Hence the only honest caveat about the outcome: a good method does not guarantee winning a matter or escaping a penalty, because that never rests on the firm alone. What is guaranteed is that the one who decides and the one who answers for it is a lawyer, not a machine.

SECTION 05

If you are audited

The previous section answers whether the way the firm handles your information is defensible. There is a second, more specific question, asked above all by the client that is a company or that has compliance obligations of its own: what can your lawyer hand over so that you are the one able to account for things on the day your auditor, your data protection officer or an authority asks you about the chain of processing of your data.

5.1 Why this affects you as a client

If you are a company, you are the controller of the data you handle, so your responsibility does not stop at the door of the law firm to which you entrust the matter. The GDPR requires you to act with diligence and to be able to demonstrate it — this is the accountability principle of arts. 5.2 and 24 — including when you entrust your data to a professional who is going to handle it with artificial intelligence. That means that, if the moment comes, you will have to be able to show that this chain of processing offers sufficient safeguards — and saying so is not enough. Art. 28 of the GDPR goes a step further: it is the data processing agreement that binds the firm to the provider of the tool, and it forms part of what your lawyer can show to anyone who audits you. A lawyer who is alert to this does not leave you to fend for yourself on the point, but gives you the means to document it.

5.2 The package your lawyer can produce

Without going into the inner workings of the system, what the firm can make available to you, or show to anyone who audits you, comes down to five things:

- **The data processing agreement** (art. 28 of the GDPR) with the provider of the tool, including the commitment not to use your data to train its models.
- **The record of processing activities** (art. 30 of the GDPR), which documents what data is processed, for what purpose and on what basis.
- **The technical and organisational measures in writing** (arts. 24 and 32 of the GDPR), that is, the concrete safeguards that protect the information, not a generic declaration of good intentions.
- **The separation of the most sensitive material**, which by its nature does not even enter the artificial intelligence and is kept encrypted outside the cloud.
- **The history of each action**, which makes it possible to reconstruct how a matter was handled if anyone asks.

5.3 What all of that demonstrates

What the law values is not that an incident never happened, but the diligence with which the work was done before one could (the accountability principle of art. 5.2 of the GDPR). A lawyer who produces the agreement, the record, the written measures and the history leaves you in a better position than one who merely declares themselves careful: the first is evidence, the second is just words. When it is your lawyer who supplies that evidence, it shores up your own diligence in the eyes of whoever audits you.

5.4 The commitment, without overstating it

From that same principle comes the only honest promise that can be made:

> *You are not promised "guaranteed compliance" or "immunity from the authority". The work is carried out with processing aligned with GDPR good practice, and the documentation that evidences diligence — yours and the firm's — is kept. The final assessment always rests with the supervisory authority.*

SECTION 06

Frequently asked questions

The questions that come up most often once a client knows that their lawyer works with artificial intelligence.

6.1 About your information

Has my data been put into ChatGPT or a similar tool?

No. Your material is not pasted into a general-purpose service, where data drops out of sight and may end up reused or fed into the training of models. It is handled within a professional environment, under a data processing agreement and a commitment not to train on it; the most sensitive material does not even enter the tool.

Who can see my file?

The firm, as always. The information lives within its own environment, with no central server pooling it with that of other clients or firms: that pooling is precisely what would multiply the risk of something being crossed over or leaked.

Can I ask for artificial intelligence not to be used on my matter?

Yes. It is your information, and the final say on how it is handled is yours. It is worth knowing, though, that the use described here is designed precisely to protect it better than working on tools that carry no safeguards.

6.2 About reliability

What if the tool gets something wrong or "makes up" a citation in my case?

That is exactly what the method guards against: no citation is taken as sound simply for appearing in the answer. Every reference is checked against the official source and, if it cannot be verified, it is flagged and stopped rather than presented as settled.

Does a machine decide how my case is handled?

No. The tool proposes and organises work; it does not choose the strategy, it does not weigh the evidence and it does not assume legal judgement. The last word always rests with your lawyer, who is the one who decides and the one who is accountable.

6.3 About guarantees

Does this guarantee that I will win, or that I won't be penalised?

No, and no honest person should promise you that: the outcome never depends on the firm alone. What the system provides is less exposure to error and a documented record that the work was done with diligence — which is a different thing from guaranteeing an outcome.

Does it cost me more?

It is not a separate charge. Artificial intelligence is one of the firm's working tools, just as a legal database or office supplies are, and its purpose is to save time on the mechanical work so as to devote it to what calls for judgement.

SECTION 07

Bibliography and sources

This dossier is for general information, but what it describes rests on a specific body of legislation and a specific contractual framework. The principal references are gathered here, in case you wish to check them or take them to whoever advises you on data protection.

7.1 Legislation

- Regulation (EU) 2016/679, the General Data Protection Regulation (GDPR), in particular articles 5.2 (accountability), 24 and 32 (technical and organisational measures), 28 (processor) and 30 (record of processing activities).
- Organic Law 3/2018, of 5 December, on the Protection of Personal Data and the guarantee of digital rights (LOPDGDD).
- General Statute of the Spanish Legal Profession (Royal Decree 135/2021, of 2 March), in particular its art. 21 (the lawyer's duty of professional secrecy).

7.2 Contractual framework of the processing

- The commercial terms of the professional-use artificial intelligence provider and its data processing agreement (art. 28 GDPR), with the commitment not to train its models on the client's data.

7.3 What the firm relies on internally

- A proprietary suite of legal sources (BOE legislation, official case law and authoritative guidance), with their own updating routines, against which citations are checked.
- The firm's governance documentation, which includes the protocol for the use of artificial intelligence, the record of processing activities and the record of technical and organisational measures.

> *The legislative references are cited by their current official designation. The wording applicable to a particular matter is always checked as at the date of the events, since that is the wording that governs — not necessarily today's version.*